UiO : Matematisk institutt
Det matematisk-naturvitenskapelige fakultet

Bombieri-Vinogradovs teorem og primtallsgap

Mats Myhr Hansen

Masteroppgave, høsten 2015

Sammendrag

Denne oppgaven er inspirert av Zhang Yitangs gjennombrudd for primtallsgap i 2013. Hovedpoenget i denne oppgaven er å bevise Bombieri-Vinogradovs teorem. Dette teoremet omhandler primtallenes fordeling over et gjennomsnitt av restklasser, og det står sentralt i arbeidet med primtallsgap. Beviset i denne oppgaven følger [Har11], og er ment som en utfyllende og mer forklarende tekst. Vi begynner med en kort introduksjon om primtall og primtallenes fordeling, før vi går igang med hoveddelen av oppgaven som er beviset av Bombieri-Vinogradovs teorem. Dirichlet-karakterer er en viktig del av beviset, så denne teorien har fått sitt eget avsnitt. Avslutningsvis vil vi diskutere Zhangs resultat og det som har skjedd i studiet av primtallsgap den siste tiden. Vi konsentrerer oss i denne oppgaven kun om nedre begrensninger av primtallsgapene, de øvrige begrensningene er en helt annen historie.

Innhold

1 Innledning **4**
- 1.1 Notasjon . . . 4
- 1.2 Fordelingen av primtall . . . 5

2 Bombieri-Vinogradovs teorem **8**
- 2.1 Den additive store såld . . . 8
- 2.2 Den multiplikative store såld . . . 17
  - 2.2.1 Karakterer på en endelig abelsk gruppe . . . 18
    - 2.2.1.1 Ortogonalitetsrelasjonene . . . 19
  - 2.2.2 Dirichlet-karakterer . . . 21
- 2.3 Beviset for Bombieri-Vinogradovs teorem . . . 25

3 Primtallsgap **44**
- 3.1 Goldston-Pintz-Yildirim . . . 44
- 3.2 Zhangs arbeid . . . 45
- 3.3 Polymath og Maynard . . . 46
- 3.4 Selbergs paritetsproblem . . . 47

Takk til

Det er mange jeg har lyst til å takke i forbinnelse med denne oppgaven. Den største takken går til min veileder professor Geir Ellingsrud som har vært svært behjelpelig og tålmodig igjennom denne til tider krevende prosessen. Mest av alt takker jeg ham for hans glede og entusiasme som har vært en motiverende faktor i alt arbeidet. Jeg vil også rette en takk til matematikkforeleserene jeg har hatt på universitetet, forelesnignene har som regel vært upåklagelige. Kanskje spesielt Helmer Aslaksen og utsagnet «math is not a spectator sport» fortjener å nevnes. Takk til Latex-protesjèet Martin Helsø for at denne oppgaven ser sånn noenlunde bra ut, og takk til Live Næss Killingland for sårt tiltrengt korrekturlesing. Takk til alle venner og bekjente jeg har opparbeidet meg over fem år på Blindern, dere har gjort studietiden til en veldig fin periode for min del. Sist, men ikke minst, vil jeg takk min matematiske «partner in crime» Ståle Zerener Haugnæss.

Kapittel 1

Innledning

1.1 Notasjon

Igjennom denne oppgaven vil $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ henholdsvis være mengden av hele, rasjonale, reelle og komplekse tall. Mengden av de naturlige tallene $\mathbb{N} = \{1, 2, 3 \ldots\}$ inneholder mengden av primtall $\mathbb{P} = \{2, 3, 5, \ldots\}$. Alle summer og produkter vil være over de naturlige tallene, om ikke annet blir oppgitt, hvor det eneste unntaket vil være summer og produkter over variabelen p, som istedenfor vil være over primtallene. Vi skriver $\sum_{s,t}$ når det er snakk om den doble summen $\sum_s \sum_t$. Vi lar $|E|$ være kardinaliteten til en endelig mengde E, og vi skriver R^* for den multiplikative gruppen av enheter for en kommutativ ring med enhet R. Lar vi a, q være heltall skriver vi $a|q$ om a deler q, og (a, q)[1] vil være største felles divisor for a og q. Om q er et naturlig tall og $a \in \mathbb{Z}$, skriver vi $a \bmod q$ (eller $a\,(mod\, q)$) om restklassen $a \bmod q \coloneqq \{a + nq \mid n \in \mathbb{Z}\}$, og vi lar $\mathbb{Z}/q\mathbb{Z}$ være ringen av slike restklasser. En aritmetisk funksjon er en funksjon fra de naturlige tallene inn i de komplekse tallene. Vi sier at en aritmetisk funksjon $f : \mathbb{N} \to \mathbb{C}$ er multiplikativ om $f(mn) = f(m)f(n)$ for alle $(m, n) = 1$, og totalt multiplikativ om vi ikke trenger betingelsen $(m, n) = 1$. I noen sammenhenger vil det være lønnsomt å heller betrakte en aritmetisk funksjon som en følge komplekse tall, hvor $a_n = f(n)$. Vi vil i denne oppgaven ha bruk for følgende aritmetiske funksjoner:

- $\pi(q)$ er primtallsfunksjonen som teller antallet primtall som er mindre eller lik q
- $\phi(q) \coloneqq |(\mathbb{Z}/q\mathbb{Z})^*|$ er Eulers phi-funksjon.
- $\tau(q) \coloneqq \sum_{d|q} 1$ er divisorfunksjonen som teller antallet positive divisorer hos q.
- $\omega(q)$ er antallet distinkte primfaktorer hos q.

[1] Denne notasjonen vil krasje med notasjonen hvor (a, b) står for det åpene intervallet fra a til b, men det vil komme klart frem av sammenhengen hvilken notasjon som menes.

- $\Omega(q)$ er antallet primfaktorer talt med multiplisitet.
- $\Lambda(q)$ er Von Mangoldt-funksjonen. $\Lambda(q)$ er $\log q$ om q er en potens av et primtall og 0 ellers.
- $\mu(q)$ er Möbius-funksjonen som er $(-1)^{\omega(q)}$ når q er kvadratfritt og 0 ellers.
- $\lambda(q)$ er Liouville-funksjonen som er $(-1)^{\Omega(q)}$.
- $I(q)$ er den konstante funksjonen 1 for alle q.
- $\epsilon(q)$ er 1 for $q = 1$ og 0 ellers.

Vi kommer i denne oppgaven til å bruke asymptotisk notasjon. Vi lar x være en stor reel parameter som man kan tenke seg går mot uendelig. Vi vil implisitt anta at x er større enn enhver fiksert konstant. Noen elementer vil være uavhengig av x og kalles fikserte elementer, men om ikke dette blir gjort klart, lar vi alle elementer vi jobber med kunne avhenge av x. For to utrykk A, B som avhenger av x sier vi at $A = O(B)$ om $|A| \leq C|B|$ for en konstant $C > 0$ (som kalles den impliserte konstanten). Dette er det samme som å si at $A \ll B$, og notasjonen $A \gg B$ betyr $B \ll A$. Om vi skriver $A \sim B$ betyr det at $\lim_{x\to\infty} A/B = 1$ og $A = o(B)$ betyr at $\lim_{x\to\infty} A/B = 0$.

1.2 Fordelingen av primtall

I mange århundrer har man studert primtall og hvordan primtallene fordeler seg blant de naturlige tallene. Allerede som 15-åring hadde Gauss brukt mye tid på å studere primtallene. Det Gauss gjorde var å telle antallet primtall i intervaller med lengde 1000. Lar vi $\pi(x)$ være antallet primtall som er mindre eller lik x, så var det en lignende funksjon som den under Gauss studerte

$$\Theta(x) := \frac{\pi(x + 500) - \pi(x - 500)}{1000}.$$

Her er $\Theta(x)$ sannsynligheten for å velge et primtall om man velger et tilfeldig heltall i området $(x-500, x+500]$. Gauss oppdaget at $\Theta(x)$ var omtrent omvendt proporsjonal med logaritmen, $\Theta(x) \approx 1/\log x$. Det er da naturlig å tenke seg at man kan få $\pi(x)$ ved å integrere $1/\log x$, altså at $\pi(x) \approx \int_2^x \frac{dt}{\log t}$. Vi bruker notasjonen $Li(x)$ for integralet over, og integralet kalles ofte Eulers logaritmiske integral. Det gikk over 100 år fra Gauss så denne sammenhengen til man hadde et resultat i boks. Det var ikke før på slutten av 1800-tallet at Hadamard og de la Valleé-Poussin uavhengig av hverandre kunne bevise det som i dag kalles Primtallsteoremet.

Teorem 1 (Primtallsteoremet)**.** *Når $x \to \infty$ har vi*

$$\pi(x) \sim Li(x).$$

Tidligere på 1800-tallet hadde Dirichlet bevist at for alle inbyrdisk primske heltall a, q, så finnes det uendelig mange primtall som er kongruent $a \pmod q$. Det finnes et tilsvarende resultat som primtallsteoremet for fordelingen av primtall i aritmetisk progresjon, igjen bevist av de la Valleé-Poussin.

Teorem 2 (Primtallsteoremet for aritmetisk progresjon)**.** *Når $x \to \infty$ har vi for fast q*

$$\pi(x; q, a) \sim \frac{1}{\phi(q)} Li(x)$$

hvor $\pi(x; q, a) = \#\{p \leq x \mid p \equiv a \pmod q\}$.

I denne oppgaven kommer vi ikke til å jobbe med $\pi(x; q, a)$, men istedet se på den nært beslektede funksjonen

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \,(mod\, q)}} \Lambda(n),$$

hvor

$$\Lambda(n) = \begin{cases} \log p & \text{hvis } n = p^k \\ 0 & \text{ellers} \end{cases}$$

er Von Mangoldt-funksjonen. Von Mangoldt-funksjonen oppfyller

$$\log(n) = \sum_{d \mid n} \Lambda(d),$$

og det er denne identiteten som knytter funksjonen opp mot primtallene, og man kan ved hjelp av Euler-summasjon oversette resultater for $\psi(x; q, a)$ til $\pi(x; q, a)$. Primtallsteoremet er ekvivalent med at $\psi(x) \sim x$, og vi har også et lignende resultat som teorem 2 for $\psi(x)$ i aritmetisk progresjon

$$\psi(x; q, a) \sim \frac{x}{\phi(q)}.$$

Det er naturlig å spørre seg hvor hvor stort feilleddet kan bli her. Et forsøk på å estimere dette ble gjort av Arnold Walfisz[Wal36] da han ved hjelp av Siegels teorem kom frem til det som i dag kalles Siegel-Walfisz teorem.

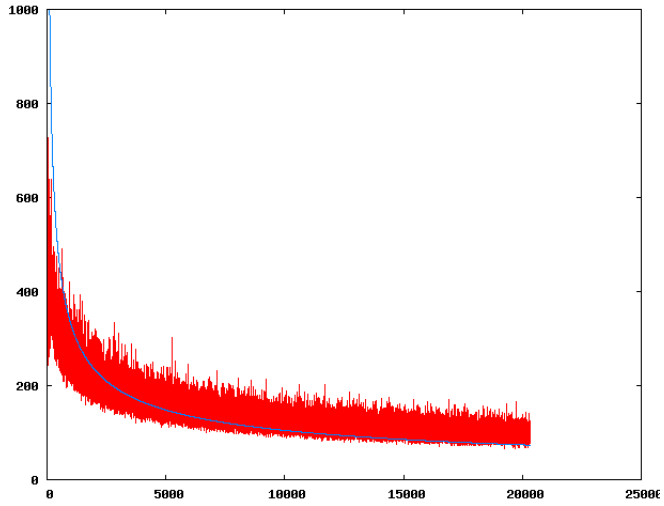
Teorem 3 (Siegel-Wafisz' teorem)**.** *La $q \geq 1, (a, q) = 1$ og $A > 0$. Da har vi*

$$\psi(x; q, a) = \frac{x}{\phi(q)} + O(x \log^{-A} x)$$

hvor den implisitte konstanten bare avhenger av A, men ikke er numerisk beregnelig.

Dette feilledet er dog langt større enn det vi forventer å være det korrekte. Om man antar den generaliserte Riemann-hypotesen kan man redusere feilledet med omtrent størrelsesorden $\sqrt{x}$, slik at

$$\psi(x; q, a) = \frac{x}{\phi(q)} + O\left(\sqrt{x} \log^2 x\right) \tag{1.1}$$



Figur 1.1: Numerisk beregning av $E(x;q,a)$

(se [MV07, korollar 13.8]). Dette er et godt estimat for $q \leq x^\theta$ hvis $\theta < 1/2$. For $q > x^{\frac{1}{2}}$ er derimot (1.1) dårligere enn det det trivielle estimatet vil være. For $q \leq x$ er det formodet at

$$\psi(x;q,a) = \frac{x}{\phi(q)} + O_\epsilon(x^{1/2+\epsilon}/q^{1/2}) \tag{1.2}$$

holder. Vi har gjort en enkel numerisk beregning for å illustrere hva som kanskje er fornuftig å forvente seg for store verdier av q. Vi har beregnet

$$\max_{(a,q)=1} \left|\psi(x;q,a) - \frac{x}{\phi(q)}\right|, \tag{1.3}$$

for $x = 10^6$ med $q \leq x^{5/7}$, og plottet dette mot $x^{1/2+\epsilon}/\sqrt{q}$ for $\epsilon = \frac{1}{6}$. Figur(1.1) gir oss en liten indikasjon på at (1.2) kan være en fornuftig hypotese, selv om man skal være forsiktig med å trekke de store konklusjonen ut av et så lite utvalg. Et bevis for enten (1.1) eller (1.2) ser fortsatt ut til å ligge langt frem i tid, så matematikere har naturlig nok kikket i andre retninger for å kontrollere dette feilleddet. Bombieri-Vinogradovs teorem ble da det neste store resultatet etter Siegel-Walfisz' teorem i denne sammenhengen. Istedenfor å se på en enkelt restklasse, ser man i Bombieri-Vinogradovs teorem på et gjennomsnitt over restklasser. Enkelt sagt så sier teoremet at feilleddet oppfører seg slik som Riemann-hypotesen forventer at det skal gjøre om man ser på gjennomsnittet over primitive restklasser opp til en viss grense, selv om det for enkelte restklasser kan se «stygt» ut.

Kapittel 2

Bombieri-Vinogradovs teorem

Teorem 4 (Bombieri-Vinogradovs teorem)**.** *La $A > 0$ være fiksert. Da har vi*

$$\sum_{q \leq Q} \max_{(a,q)=1} |E(x;q,a)| \ll_A x \log^{-A} x \tag{2.1}$$

hvor $E(x;q,a) = \psi(x;q,a) - \frac{x}{\phi(q)}$, og $Q = x^{1/2} \log^{-B} x$ for $B(A) = 2A + 8$.

Det tok nesten 30 år fra man hadde Siegel-Walfisz' teorem til Enrico Bombieri [Bom65] og Askold Ivanovich Vinogradov [Vin65] midt på 1960-tallet uavhengig av hverandre [1] beviste det som i dag kalles Bombieri-Vinogradovs teorem. Mark Barban hadde et par år tidligere begynt å se på gjennomsnittet av fordelingen av primtall i aritmetisk progresjon, og han får kanskje ufortjent lite skryt i denne sammenhengen. Beviset for Bombieri-Vinogradovs teorem bygger i stor grad på «Store såld»-ulikheter. Dette er teknikker som ble utleddet fra den russiske tallteoretikeren Yuri Linnik sine orginale ideer, som senere har blitt svært sentrale i analytisk tallteori. Navnet er dog misledende, da teknikkene har lite med matematiske sålder å gjøre. I første del av beviset opparbeider vi oss den additive store såld hvor vi arbeider med additive karakterer på formen $e(z) = \exp(2\pi i z)$ (det vil senere bli gjort klart hva en additiv karakter er). Deretter fortsetter vi med den den multiplikative store såld, hvor det som navnet foreslår, er multiplikative karakterer (Dirichlet-karakterene) som står i fokus. Avslutningsvis vil vi dele Von-Mangoldt funksjonen opp i flere deler, og estimere delene separat. Vi vil ha bruk for flere identiteter for funksjonen, og begreper som Dirichlet-konvulsjon vil være svært nyttig.

Vi går nå igang med beviset for 4, og det første vi vil opparbeide oss er den additive store såld.

[1] Vinogradov med $Q = x^{1/2-\epsilon}$, Bombieri med $Q = x^{1/2} \log^{-B} x$

2.1 Den additive store såld

Teorem 5 (Den additive store såld)**.** *La a_n være en endelig følge komplekse tall og la M og N være naturlige tall slik at $n \in \{M+1, ..., M+N\}$. Da har vi følgende*

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{an}{q}\right) \right|^2 \leq (Q^2 + N - 1)||\vec{a}||^2 \tag{2.2}$$

hvor $||\vec{a}||^2 = \sum_{M+1 \leq n \leq M+N} a_n \overline{a_n}$.

Dette estimatet er det beste mulige av denne typen, og resultatet slik som det er gitt her ble først bevist av Selberg[Sel91] og uavhenging av Montgomery og Vauhan[MV74]. Før vi kan gå i gang med å bevise teorem 5, trenger vi å opparbeide oss noen lemma. Essensen i beviset er å vise at for tall som ikke er klumpet for mye sammen, vil ikke summen over de additive karakterene bli for stor. Vi tar med oss Cauchy–Schwarz' ulikhet som vil være til stor hjelp oppgaven igjennom.

$$\left| \sum_{i=1}^{n} x_i \overline{y}_i \right|^2 \leq \sum_{i=1}^{n} |x_i|^2 \sum_{i=1}^{n} |y_i|^2. \tag{2.3}$$

Vårt første lemma vil være en generalisering av Hilberts ulikhet.

Lemma 6. *Anta at λ_r er forskjellige reelle tall hvor $|\lambda_r - \lambda_s| \geq \delta$ om $r \neq s$ for $0 < \delta < \frac{1}{2}$. Da har man for komplekse tall z_r*

$$\left| \sum_{\substack{(r,s) \\ r \neq s}} \frac{z_r \overline{z_s}}{\lambda_r - \lambda_s} \right| \leq \frac{\pi}{\delta} \sum_r |z_r|^2. \tag{2.4}$$

Bevis. Først rangerer vi λ_r-ene slik at $\lambda_1 < \lambda_2 < \lambda_3 < \dots$. Da kan vi forandre betingelsen $|\lambda_r - \lambda_s| \geq \delta$ til $|\lambda_r - \lambda_s| \geq \delta\,|r - s|$. Det første vi så vil vise er

$$\sum_r \left| \sum_{s \neq r} \frac{\overline{z_s}}{\lambda_r - \lambda_s} \right|^2 \leq \frac{\pi^2}{\delta^2} \sum_r |z_r|^2. \tag{2.5}$$

Vi har at

$$\sum_r \left| \sum_{s \neq r} \frac{\overline{z_s}}{\lambda_r - \lambda_s} \right|^2 = \sum_{(s,t)} \overline{z_s} z_t \sum_{r \neq s,t} \frac{1}{(\lambda_r - \lambda_s)(\lambda_r - \lambda_t)}, \tag{2.6}$$

som følger av

$$\left| \sum_s f(s) \right|^2 = \Big(\sum_s f(s) \Big) \overline{\Big(\sum_t f(t) \Big)} = \Big(\sum_s f(s) \Big) \Big(\sum_t \overline{f(t)} \Big) = \sum_s \sum_t f(s) \overline{f(t)}.$$

Vi vil nå dele opp høyresiden i (2.6) i to ledd. Ett hvor $s = t$, og ett hvor $s \neq t$. Vi ser først på delen hvor $s = t$ og får der

$$\sum_s |z_s|^2 \sum_{r \neq s} \frac{1}{(\lambda_r - \lambda_s)^2},$$

mens vi for delen der $s \neq t$ har

$$\begin{aligned}\sum_{\substack{(s,t)\\ s\neq t}} \overline{z_s} z_t \sum_{r \neq s,t} \frac{1}{(\lambda_r - \lambda_s)(\lambda_r - \lambda_t)} &= \sum_{\substack{(s,t)\\ s\neq t}} \frac{\overline{z_s} z_t}{\lambda_s - \lambda_t} \sum_{r \neq s,t} \left(\frac{1}{\lambda_r - \lambda_s} - \frac{1}{\lambda_r - \lambda_t} \right) \\ &= \sum_{\substack{(s,t)\\ s\neq t}} \frac{\overline{z_s} z_t}{\lambda_s - \lambda_t} \left[\sum_{r \neq s} \frac{1}{\lambda_r - \lambda_s} - \sum_{r \neq t} \frac{1}{\lambda_r - \lambda_t} + \frac{2}{\lambda_s - \lambda_t} \right].\end{aligned}$$

Når vi nå summerer over alle s, t så vil summene $\sum_{r \neq s} \frac{1}{\lambda_r - \lambda_s}$ og $\sum_{r \neq t} \frac{1}{\lambda_r - \lambda_t}$ kansellere hverandre og vi står igjen med

$$\sum_{\substack{(s,t)\\ s\neq t}} \frac{\overline{z_s} z_t}{\lambda_s - \lambda_t} \left[\frac{2}{\lambda_s - \lambda_t} \right] = \sum_{\substack{(s,t)\\ s\neq t}} \frac{2\overline{z_s} z_t}{(\lambda_s - \lambda_t)^2}.$$

Vi bruker nå at $2|z_s z_t| \leq |z_s|^2 + |z_t|^2$ og får

$$\left| \sum_{\substack{(s,t)\\ s\neq t}} \frac{2\overline{z_s} z_t}{(\lambda_s - \lambda_t)^2} \right| \leq \sum_s \sum_{t \neq s} \frac{|z_s|^2 + |z_t|^2}{(\lambda_s - \lambda_t)^2} = 2 \sum_s |z_s|^2 \sum_{t \neq s} \frac{1}{(\lambda_s - \lambda_t)^2},$$

hvor den siste likheten her kommer av at ethvert par (i, j) opptrer to ganger, en gang hvor $i = s$, $j = t$ og en gang hvor $i = t$, $j = s$. Setter vi nå sammen delen hvor $s = t$ og delen hvor $s \neq t$ får vi

$$\begin{aligned}\sum_r \left| \sum_{r \neq s} \frac{\overline{z_s}}{\lambda_r - \lambda_s} \right|^2 &= \sum_s |z_s|^2 \sum_{r \neq s} \frac{1}{(\lambda_r - \lambda_s)^2} + 2 \sum_s |z_s|^2 \sum_{t \neq s} \frac{1}{(\lambda_s - \lambda_t)^2} \\ &= 3 \sum_s |z_s|^2 \sum_{r \neq s} \frac{1}{(\lambda_r - \lambda_s)^2}.\end{aligned}$$

Betingelsen $|\lambda_r - \lambda_s| \geq \delta |r - s|$ gir oss at

$$\begin{aligned}3 \sum_s |z_s|^2 \sum_{r \neq s} \frac{1}{(\lambda_r - \lambda_s)^2} &\leq \frac{3}{\delta^2} \sum_s |z_s|^2 \sum_{r \neq s} \frac{1}{(r - s)^2} \\ &\leq \frac{3}{\delta^2} \sum_s |z_s|^2 \left(2 \sum_{n=1}^{\infty} \frac{1}{n^2} \right) = \frac{6}{\delta^2} \frac{\pi^2}{6} \sum_s |z_s|^2 \\ &= \frac{\pi^2}{\delta^2} \sum_s |z_s|^2,\end{aligned}$$

og vi har (2.5). Hvis vi avslutningsvis bruker Cauchy–Schwarz' ulikhet på venstresiden i (2.4) og slår dette sammen med (2.5) ender vi opp med

$$\left|\sum_{\substack{(r,s)\\ r\neq s}} \frac{z_r\overline{z_s}}{\lambda_r-\lambda_s}\right|^2 \leq \sum_r |z_r|^2 \sum_r \left|\sum_{s\neq r} \frac{\overline{z_s}}{\lambda_r-\lambda_s}\right|^2$$

$$\leq \sum_r |z_r|^2 \left(\frac{\pi^2}{\delta^2}\sum_r |z_r|^2\right) = \left(\frac{\pi}{\delta}\sum_r |z_r|^2\right)^2,$$

som gir oss lemmaet vi var ute etter. □

Før vi går videre trenger vi et lemma fra kompleks funksjonsteori, samt en ny definisjon.

Lemma 7. *Hvis z er et komplekst tall og $z \notin \mathbb{Z}$ vil*

$$\frac{1}{z} + 2z\sum_{k=1}^{\infty} \frac{(-1)^k}{z^2-k^2} = \frac{\pi}{\sin \pi z}. \tag{2.7}$$

Bevis. Se [Ahl66, Side 188]. □

Definisjon. La $||x||$ være avstanden fra x til nærmeste heltall. Om $0 < \delta < \frac{1}{2}$ sier vi at tallene $\alpha_r \in \mathbb{R}$ er δ-plasserte hvis$||\alpha_r - \alpha_s|| \geq \delta$ for alle $r \neq s$. Det finnes maksimalt $1 + \delta^{-1}$ slike distinkte α_r.

Dette gir oss følgende korollar.

Korollar 8. *For komplekse tall z_r og δ-plasserte α_r har vi*

$$\left|\sum_{\substack{(r,s)\\ r\neq s}} \frac{z_r\overline{z_s}}{\sin \pi(\alpha_r-\alpha_s)}\right| \leq \delta^{-1}\sum_r |z_r|^2.$$

Bevis. Vi benytter oss av lemma 6 med $z_{m,r} = (-1)^m z_r$ og $\lambda_{m,r} = m + \alpha_r$ for $1 \leq m \leq K$. Dette gir oss

$$\begin{aligned}\left|\sum_{\substack{(r,m),(s,n)\\ (r,m)\neq(s,n)}} (-1)^{m-n}\frac{z_r\overline{z_s}}{m-n+\alpha_r-\alpha_s}\right| &= \left|\sum_{\substack{(r,m),(s,n)\\ (r,m)\neq(s,n)}} \frac{z_{m,r}\overline{z_{n,s}}}{\lambda_{m,r}-\lambda_{n,s}}\right| \\ &\leq \frac{\pi}{\delta}\sum_r |z_{m,r}|^2 \leq \frac{\pi K}{\delta}\sum_r |z_r|^2.\end{aligned} \tag{2.8}$$

Om vi nå ser på venstresiden i (2.8) for tilfellet hvor $r = s$ og fokuserer på leddet i summen med $m = i$, $n = j$, ser vi at $(-1)^{i-j}\frac{|z_r|^2}{i-j} = -(-1)^{j-i}\frac{|z_r|^2}{j-i}$. Dette betyr at leddene med $m = j$, $n = i$ har motsatt fortegn av leddene med

$m = i$, $n = j$. Disse leddene vil da kansellere hverandre, og vi kan da forenkle betingelsen fra $(r, m) \neq (s, n)$ til $r \neq s$. Derfor vil

$$\frac{\pi}{\delta} \sum_r |z_r|^2 \geq \frac{1}{K} \Big| \sum_{\substack{r,s,m,n \\ r \neq s}} (-1)^{m-n} \frac{z_r \overline{z_s}}{m - n + \alpha_r - \alpha_s} \Big|$$

$$= \Big| \sum_{\substack{r,s \\ r \neq s}} z_r \overline{z_s} \sum_{k=-K}^{K} \frac{N(k)}{K} \frac{(-1)^k}{k + \alpha_r - \alpha_s} \Big|,$$

hvor $N(k)$ er antallet par (m, n) med $1 \leq m, n \leq K$ slik at $m - n = k$. Bruker vi nå at $N(k) = K - |k|$ (for $|k| \leq K$) får vi

$$\frac{\pi}{\delta} \sum_r |z_r|^2 \geq \Big| \sum_{\substack{r,s \\ r \neq s}} z_r \overline{z_s} \sum_{k=-K}^{K} \Big(1 - \frac{|k|}{K}\Big) \frac{(-1)^k}{k + \alpha_r - \alpha_s} \Big|. \tag{2.9}$$

$$= \Big| \sum_{\substack{r,s \\ r \neq s}} z_r \overline{z_s} \sum_{k=-K}^{K} \frac{(-1)^k}{k + \alpha_r - \alpha_s} - \sum_{\substack{r,s \\ r \neq s}} z_r \overline{z_s} \sum_{k=-K}^{K} \frac{|k|}{K} \frac{(-1)^k}{k + \alpha_s - \alpha_s} \Big|$$

$$\geq \Big| \Big| \sum_{\substack{r,s \\ r \neq s}} z_r \overline{z_s} \sum_{k=-K}^{K} \frac{(-1)^k}{k + \alpha_r - \alpha_s} \Big| - \Big| \sum_{\substack{r,s \\ r \neq s}} z_r \overline{z_s} \sum_{k=-K}^{K} \frac{|k|}{K} \frac{(-1)^k}{k + \alpha_s - \alpha_s} \Big| \Big|, \tag{2.10}$$

hvor vi i siste steg her har brukt den omvendte trekantulikheten. Setter vi $z = \alpha_r - \alpha_s$ har vi for den første indre summen

$$\begin{aligned} \sum_{k=-K}^{K} \frac{(-1)^k}{k+z} &= \frac{1}{z} + \sum_{k=-K}^{-1} \frac{(-1)^k}{k+z} + \sum_{k=1}^{K} \frac{(-1)^k}{k+z} = \frac{1}{z} + \sum_{k=1}^{K} \Big(\frac{(-1)^{-k}}{-k+z} + \frac{(-1)^k}{k+z} \Big) \\ &= \frac{1}{z} + 2z \sum_{k=1}^{K} \frac{(-1)^k}{z^2 - k^2}, \end{aligned}$$

og tilsvarende for den andre

$$\sum_{k=-K}^{K} \frac{|k|}{K} \frac{(-1)^k}{k + \alpha_r - \alpha_s} = \frac{1}{Kz} + \frac{2z}{K} \sum_{k=1}^{K} \frac{|k|(-1)^k}{z^2 - k^2} = \frac{1}{Kz} + \frac{2z}{K} \sum_{k=1}^{K} k \frac{(-1)^k}{z^2 - k^2}.$$

Vi vil nå argumentere for at uttrykket over forsvinner om vi lar $K \to \infty$. Tar vi med summen over r, s fra (2.10) har vi

$$\Big| \sum_{\substack{r,s \\ r \neq s}} z_r \overline{z_s} \Big(\frac{1}{Kz} + \frac{2z}{K} \sum_{k=1}^{K} k \frac{(-1)^k}{z^2 - k^2} \Big) \Big| = \Big| \sum_{\substack{r,s \\ r \neq s}} z_r \overline{z_s} \Big| \Big| \frac{1}{Kz} + \frac{2z}{K} \sum_{k=1}^{K} k \frac{(-1)^k}{z^2 - k^2} \Big|,$$

hvor vi for det siste leddet oppfyller ulikheten

$$\left|\frac{1}{Kz}+\frac{2z}{K}\sum_{k=1}^{K}k\frac{(-1)^k}{z^2-k^2}\right|\leq\frac{1}{K|z|}+\frac{2|z|}{K}\sum_{k=1}^{K}\frac{k}{|z^2-k^2|}.$$

Her vil z være fast mens k øker. Det vil da finnes $N\in\mathbb{N}$ slik at $|z^2-k^2|\geq\frac{1}{2}k^2$ for alle $k\geq N$, og vi kan da skrive om slik at vi har

$$\begin{aligned}&\frac{1}{K|z|}+\frac{2|z|}{K}\sum_{k=1}^{N}(-1)^k\frac{k}{|z^2-k^2|}+\frac{2|z|}{K}\sum_{k=N+1}^{K}(-1)^k\frac{k}{|z^2-k^2|}\\&\leq\frac{1}{K|z|}+\frac{2|z|}{K}\sum_{k=1}^{N}(-1)^k\frac{k}{|z^2-k^2|}+\frac{2|z|}{K}\sum_{k=N+1}^{K}\frac{k}{\frac{1}{2}k^2}\\&=\frac{1}{K|z|}+\frac{2|z|}{K}\sum_{k=1}^{N}(-1)^k\frac{k}{|z^2-k^2|}+\frac{4|z|}{K}\sum_{k=N+1}^{K}\frac{1}{k}.\end{aligned}$$

For K som går mot uendelig vil åpenbart de to første leddene her falle bort, mens vi for det siste leddet minner om at

$$\sum_{k=N+1}^{K}\frac{1}{k}\sim\log(K)$$

når $K\to\infty$. Samtidig vet vi at $\log(K)=o(K)$, som betyr at vi i (2.10) kun vil stå igjen med

$$\begin{aligned}&=\left|\sum_{\substack{r,s\\r\neq s}}z_r\overline{z_s}\sum_{k=-K}^{k}\frac{(-1)^k}{k+z}\right|=\left|\sum_{\substack{r,s\\r\neq s}}z_r\overline{z_s}\left(\frac{1}{z}+2z\sum_{k=1}^{K}\frac{(-1)^k}{z^2-k^2}\right)\right|\\&=\left|\sum_{\substack{r,s\\r\neq s}}z_r\overline{z_s}\frac{\pi}{\sin\pi z}\right|,\end{aligned}$$

hvor den siste likheten følger av lemma 7. Vi har da vist at

$$\left|\sum_{\substack{r,s\\r\neq s}}z_r\overline{z_s}\frac{\pi}{\sin\pi z}\right|\leq\frac{\pi}{\delta}\sum_r|z_r|^2$$

og vi er i mål. □

Dette korollaret gir oss direkte et nytt korollar.

Korollar 9. *For ethvert reelt tall x, komplekse tall z_r og δ-plasserte α_r har vi*

$$\left|\sum_{\substack{(r,s)\\r\neq s}}\frac{z_r\overline{z_s}\sin 2\pi x(\alpha_r-\alpha_s)}{\sin\pi(\alpha_r-\alpha_s)}\right|\leq\delta^{-1}\sum_r|z_r|^2.$$

Bevis. Bruker vi korollar 8 først med $z_r' = z_r e(x\alpha_r)$ og så med $z_r'' = z_r e(-x\alpha_r)$, samtidig som vi bemerker at $|z_r'| = |z_r''| = |z_r|$ får vi henholdsvis

$$\left| \sum_{\substack{(r,s)\\ r\neq s}} \frac{z_r\overline{z_s}e(x\alpha_r - x\alpha_s)}{\sin\pi(\alpha_r-\alpha_s)} \right| \leq \delta^{-1}\sum_r |z_r|^2$$

og

$$\left| \sum_{\substack{(r,s)\\ r\neq s}} \frac{z_r\overline{z_s}e(-x\alpha_r + x\alpha_s)}{\sin\pi(\alpha_r-\alpha_s)} \right| \leq \delta^{-1}\sum_r |z_r|^2.$$

Tar vi nå med oss at $e(z) - e(-z) = 2i\sin(2\pi z)$ kan vi avslutningsvis få

$$\begin{aligned}
& \left| \sum_{\substack{(r,s)\\ r\neq s}} \frac{z_r\overline{z_s}\sin 2\pi x(\alpha_r-\alpha_s)}{\sin\pi(\alpha_r-\alpha_s)} \right| \\
= & \left| \sum_{\substack{(r,s)\\ r\neq s}} \frac{z_r\overline{z_s}\Big(e(x(\alpha_r-\alpha_s)) - e(x(-\alpha_r+\alpha_s))\Big)}{2i\sin\pi(\alpha_r-\alpha_s)} \right| \\
\leq & \frac{1}{2}\left| \sum_{\substack{(r,s)\\ r\neq s}} \frac{z_r\overline{z_s}e(x\alpha_r - x\alpha_s)}{\sin\pi(\alpha_r-\alpha_s)} \right| + \frac{1}{2}\left| \sum_{\substack{(r,s)\\ r\neq s}} \frac{z_r\overline{z_s}e(-x\alpha_r + x\alpha_s)}{\sin\pi(\alpha_r-\alpha_s)} \right| \\
\leq & \delta^{-1}\sum_r |z_r|^2.
\end{aligned}$$

□

Det vi nå trenger er et dualitetsprinsipp for bilineære former slik at vi har lov til å bytte rekkefølgen for summasjonen i teorem 5.

Lemma 10 (Dualitets-lemma)**.** *Gitt en funksjon $\phi(m,n)$ anta at vi for enhver følge komplekse tall β_n har*

$$\sum_m \left| \sum_n \beta_n\phi(m,n) \right|^2 \leq \Delta||\vec{\beta}||^2, \tag{2.11}$$

da vil vi for enhver kompleks følge α_n og samme Δ ha

$$\sum_n \left| \sum_m \alpha_m\phi(m,n) \right|^2 \leq \Delta||\vec{a}||^2.$$

Bevis. Lar vi $\beta_n = \sum_m \overline{\alpha_m\phi(m,n)}$ har vi

$$\sum_n \left| \sum_m \alpha_m\phi(m,n) \right|^2 = \sum_n \Big(\sum_m \alpha_m\phi(m,n) \Big) \Big(\sum_l \overline{\alpha_l\phi(l,n)} \Big)$$

$$= \sum_n \sum_m \alpha_m \beta_n \phi(m,n) = \sum_m \alpha_m \sum_n \beta_n \phi(m,n).$$

Kaller vi nå den siste summen ovenfor for $\Phi(m,n)$ og bruker Cauchy–Schwarz' ulikhet sammen med antakelsen i (2.11), så har vi

$$|\Phi(m,n)|^2 \leq \sum_m |\alpha_m|^2 \sum_m \left| \sum_n \beta_n \phi(m,n) \right|^2 \leq \Delta ||\vec{a}||^2 ||\vec{\beta}||^2. \tag{2.12}$$

Vi har valgt β_n slik at

$$\Phi(m,n) = \sum_n \left| \sum_m \alpha_m \phi(m,n) \right|^2 = \sum_n |\beta_n|^2 = ||\vec{\beta}||^2,$$

og at $\Phi(m,n) \leq \Delta ||\vec{a}||^2$ følger da av (2.12). □

Nå trenger vi et siste lemma som vi for enkelhets skyld deler opp i to deler. Teorem 5 vil da falle ut som et korollar om vi velger α_r-ene til å være rasjonale tall, som vi viser er separert godt nok fra hverandre.

Lemma 11. *For enhver kolleksjon δ-plasserte α_r og alle komplekse tall a_n med $M < n \leq M+N$ har vi*

(*a*)

$$\sum_r \left| \sum_{M<n<M+N} a_n e(\alpha_r n) \right|^2 \leq (\delta^{-1} + N) ||\vec{a}||^2.$$

(*b*) *Vi kan erstatte $(\delta^{-1}+N)$ med $(\delta^{-1}+N-1)$.*

Bevis. (*a*) Ved dualitet er det nok å bevise.

$$\sum_{N=n+1}^{M+N} \left| \sum_r z_r e(\alpha_r n) \right|^2 \leq (\delta^{-1}+N) \|\vec{z}\|^2.$$

Vi skriver først om venstresiden til

$$\sum_{N=M+1}^{M+N} \left(\sum_r z_r e(\alpha_r n) \right) \left(\sum_s \overline{z_s} e(-\alpha_s n) \right).$$

For de leddene hvor $r = s$ har vi

$$\sum_{n=M+1}^{M+N} \sum_r |z_r|^2 = N ||\vec{z}||^2,$$

mens vi for leddene der $r \neq s$ har

$$\sum_{N=n+1}^{M+N} \left(\sum_r z_r e(\alpha_r n) \right) \left(\sum_{s \neq r} \overline{z_s} e(-\alpha_s n) \right)$$

$$= \sum_{\substack{(r,s)\\ r\neq s}} z_r\overline{z_s} \sum_{n=n+1}^{M+N} e(n(\alpha_r-\alpha_s)). \tag{2.13}$$

Summen for en geometrisk rekke gir oss at

$$\sum_{c<n\leq d} e(n\alpha) \quad = \quad \frac{e((c+1)\alpha)-e((d+1)\alpha)}{1-e(\alpha)}$$

$$= \frac{e((c+\frac{1}{2})\alpha)-e((d+\frac{1}{2})\alpha)}{e(-\frac{\alpha}{2})-e(\frac{\alpha}{2})}.$$

Vi har her nevneren på formen $e(z)-e(-z)$, men vi vil også ha telleren på denne formen. Vi multipliserer derfor med

$$e((c+d+1)\frac{\alpha}{2})e(-(c+d+1)\frac{\alpha}{2}) = 1,$$

og får

$$e((c+d+1)\frac{\alpha}{2})\frac{e(-(d-c)\frac{\alpha}{2})e((d-c)\frac{\alpha}{2})}{e(-\frac{\alpha}{2})-e(\frac{\alpha}{2})} = e((c+d+1)\frac{\alpha}{2})\frac{\sin(\pi(d-c)\alpha)}{\sin\pi\alpha}.$$

Setter vi nå dette inn i (2.13) har vi

$$\sum_{\substack{(r,s)\\ r\neq s}} z_r\overline{z_s}e((M+\frac{1}{2}(N+1))(\alpha_r-\alpha_s))\frac{\sin\pi N(\alpha_r-\alpha_s)}{\sin\pi(\alpha_r-\alpha_s)}.$$

Velger vi $N=2x$ og tar absoluttverdien så kan vi bruke korollar 9 slik at vi får

$$\sum_{\substack{(r,s)\\ r\neq s}} z_r\overline{z_s}e((M+\frac{1}{2}(N+1))(\alpha_r-\alpha_s))\frac{\sin\pi N(\alpha_r-\alpha_s)}{\sin\pi(\alpha_r-\alpha_s)}$$

$$\leq \quad \left|\sum_{\substack{(r,s)\\ r\neq s}} z_r\overline{z_s}\frac{\sin 2\pi x(\alpha_r-\alpha_s)}{\sin\pi(\alpha_r-\alpha_s)}\right|$$

$$\leq \quad \delta^{-1}\|\vec{z}\|^2.$$

Slår vi så sammen delen der $r=s$ med delen der $r\neq s$, får vi

$$\sum_{n=M+1}^{M+N}\left|\sum_r e(\alpha_r n)\right|^2 \leq (\delta^{-1}+N)\|\vec{z}\|^2$$

og (a) er bevist.
(b) For å kunne tjene inn en ekstra -1, trenger vi et lite knep kreditert Paul Cohen. La $a_{n,}, \alpha_r$ og δ være like som i (a). Vi setter nå $\beta_{r,k} = \dfrac{\alpha_r+k}{K}$ for

$1 \leq k \leq K$, og legger merke til at disse vil være $\frac{\delta}{K}$-plasserte. Vi kan da skrive $\alpha_r = \beta_{r,k}K - k$ slik at

$$\sum_r \left| \sum_{n=M+1}^{M+N} a_n e(\alpha_r n) \right|^2 = \sum_r \left| \sum_{n=M+1}^{M+N} a_n e(\beta_{r,k} K n) e(-kn) \right|^2.$$

Det at $e(z)$ ikke bryr seg om man legger til eller trekker fra et heltall i argumentet gjør at $e(\beta_{r,k}Kn)e(-kn) = e(B_{r,k}Kn)$ slik at vi kan summere over $\sum_{k=1}^{K}$ og bare få et bidrag på K. Dette gir oss

$$\sum_r \left| \sum_{n=M+1}^{M+N} a_n e(\beta_{r,k} K n) e(-kn) \right|^2 = \frac{1}{K} \sum_{k=1}^{K} \sum_r \left| \sum_{n=M+1}^{M+N} e(\beta_{r,k} K n) \right|^2.$$

Om vi nå setter $m = nK$ vil den indre summen være over $MK + K \leq m \leq MK + NK$, hvor det er $NK - K + 1$ ledd. Bruker vi nå (a) har vi

$$\frac{1}{K} \sum_{k=1}^{K} \sum_r \left| \sum_{m=MK+K}^{MK+NK} e(\beta_{r,k} m) \right|^2 \leq \frac{1}{K} (\delta^{-1} K + NK - K + 1) \|\vec{a}\|^2,$$

og lar vi $K \to \infty$ får vi

$$\sum_r \left| \sum_{n=M+1}^{M+N} a_n e(\alpha_r n) \right|^2 \leq (\delta^{-1} + N - 1) \|\vec{a}\|^2$$

□

Da gjenstår det bare et elementært argument før vi har den additive store såld.

Bevis for teorem 5. La α_r være de rationale tallene $\frac{a}{q}$ med $1 \leq q \leq Q$ og $(a, q) = 1$. Disse α_r-ene vil være δ-plasserte med $\delta = Q^{-2}$ fordi vi for $\frac{a}{b} \neq \frac{c}{d}$ har

$$\left|\left| \frac{a}{b} - \frac{c}{d} \right|\right| = \left|\left| \frac{ad - bc}{bd} \right|\right| \geq \left|\left| \frac{1}{bd} \right|\right| \geq Q^{-2}.$$

Bruker vi nå disse α_r-ene i lemma 11 får vi teorem 5. □

2.2 Den multiplikative store såld

Nå som vi har den additive store såld på plass er det på tide å rette fokuset mot den multiplikative store såld. Her vil fokuset være på noen totalt multiplikative funksjoner som kalles Dirichlet-karakterer.

Teorem 12 (Den multiplikative store såld)**.** *For naturlige tall M, N, la a_n være en følge komplekse tall med $n \in \{M+1, \dots, M+N\}$. Da har vi følgende*

$$\sum_{q \leq Q} \frac{q}{\phi(q)} \sideset{}{^\star}\sum_{\chi \,(mod\, q)} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \leq (Q^2 + N - 1)\|\vec{a}\|^2,$$

hvor $\sum^\star$ betyr at vi summerer over alle primitive karakter χ.

Dette resultatet stammer fra Bombieri og Davenport[BD69][2]. Før vi går igang med å bevise den multiplikative store såld, trenger vi noen resultater for Dirichlet-karakterer, men vi introduserer først generelle karakterer på abelske grupper.

2.2.1 Karakterer på en endelig abelsk gruppe

Denne biten om karkterer følger gangen i [Pol09, kapittel 3.4].

Definisjon. La G være en endelig multiplikativ abelsk gruppe og la $\mathbb{C}^*$ være gruppen av enheter i $\mathbb{C}$. En *karakter* på G er en homomorfi

$$\chi \colon G \to \mathbb{C}^*.$$

Dette vil være en funksjon fra G inn i de ikkenull komplekse tallene som oppfyller $\chi(ab) = \chi(a)\chi(b)$ for alle $a, b \in G$.

Vi lar $\hat{G}$ være mengden av alle karakterer på G, og bruker notasjonen χ_0 om den *trivielle* karakteren som er identisk lik 1. Noe som er verdt å legge merke til er at om χ er en karakter på G og vi lar $g \in G$ ha orden n, så er $\chi(g)^n = \chi(g^n) = \chi(1) = 1$. Dermed vil $\chi(g)$ være en n-te enhetsrot for alle $g \in G$ med respektiv orden n. Før vi går igang med å bevise ortogonalitetsrelasjonene som er noen de viktigste egenskapene karakterene har, trenger vi å kunne si noe om antallet karakterer.

Proposisjon 13. *For alle endelige abelske grupper G har vi $|\hat{G}| = |G|$.*

Bevis. Fundamentalteoremet for endelige abelske grupper sier at alle endelige abelske grupper er isomorfe med en direkte sum av sykliske grupper. Dette betyr at man alltid kan finne elementer $g_1, \dots, g_k \in G$ med respektive ordner $n_1, \dots n_k$, slik at alle $g \in G$ har en unik representasjon på formen

$$g_1^{e_1} g_2^{e_2} \cdots g_k^{e_k}, \tag{2.14}$$

hvor $0 \leq e_i < n_i$ for hver $1 \leq i \leq k$. Ser vi på $\chi(g)$ hvor $g = g_1^{e_1} g_2^{e_2} \cdots g_k^{e_k} \in G$ har vi

$$\chi(g) = \chi(g_1^{e_1} g_2^{e_2} \cdots g_k^{e_k}) = \chi(g_1^{e_1})\chi(g_2^{e_2}) \cdots \chi(g_k^{e_k}) = \chi(g_1)^{e_1}\chi(g_2)^{e_2} \cdots \chi(g_k)^{e_k},$$

[2] Riktignok var deres originale resultat noe svakere.

altså er alle karakterer χ på G bestemt av hvor de sender $g_1, \dots g_k$. Vi vet at $\chi(g_i)$ alltid vil være en n_i-te enhetsrot, så vi kan maksimalt ha $\prod_i^k n_i = |G|$ karakterer på G. Lar vi så η_i for hver $1 \leq i \leq k$ være en vilkårlig n_i-te enhetsrot og setter

$$\tilde{\chi}(g_1^{e_1} g_2^{e_2} \cdots g_k^{e_k}) \coloneqq \eta_1^{e_1} \eta_2^{e_2} \cdots \eta_k^{e_k},$$

har vi en ny karakter. Om vi antar at vi kan skrive g på to forskjellige måter slik at $g = g_1^{e_1} g_2^{e_2} \cdots g_k^{e_k} = g_1^{f_1} g_2^{f_2} \cdots g_k^{f_k}$, må $e_i \equiv f_i (mod\, n_i)$ og $\eta_i^{e_i} = \eta_i^{f_i}$. Dette betyr at $\tilde{\chi}$ er veldefinert. Samtidig vil

$$\begin{aligned} \tilde{\chi}(g_1^{m_1} \cdots g_k^{m_k} g_1^{n_1} \cdots g_k^{n_k}) &= \tilde{\chi}(g_1^{m_1+n_1} \cdots g_k^{m_k+n_k}) = \eta_1^{m_1+n_1} \cdots \eta_k^{m_k+n_k} \\ &= \eta_1^{m_1} \cdots \eta_k^{m_k} \eta_1^{n_1} \cdots \eta_k^{n_k} \\ &= \tilde{\chi}(g_1^{m_1} \cdots g_k^{m_k}) \tilde{\chi}(g_1^{n_1} \cdots g_k^{n_k}), \end{aligned}$$

så χ er også multiplikativ, og vi har dermed vist at det finnes $|G|$ karakterer på G. □

2.2.1.1 Ortogonalitetsrelasjonene

Vi er nå klare til å bevise ortogonalitetsrelasjonene som er vitale i beviset av den multiplikative store såld. Før vi gjør det, har vi lyst til å gjøre $\hat{G}$ om til en gruppe. Det kan vi gjør det ved å definere multiplikasjonen punktvis slik at vi for to karakterer $\chi, \psi \in \hat{G}$ setter

$$(\chi\psi)(g) \coloneqq \chi(g)\psi(g).$$

Identitetselementet vil her være χ_0 og for hver $\chi \in \hat{G}$ setter vi

$$\chi^{-1}(g) \coloneqq \chi(g)^{-1}.$$

Da alle verdier χ tar er enhetsrøtter, vil $\chi^{-1} = \overline{\chi}$ hvor $\overline{\chi}$ er definert som $\overline{\chi}(g) \coloneqq \overline{\chi(g)}$ for hver $g \in G$.

Lemma 14 (Første ortogonalitetsrelasjon)**.** *La G være en endelig abelsk gruppe og la χ,ψ være to karakterer på G. Da har vi*

$$\sum_{g \in G} \overline{\chi}(g)\psi(g) = \begin{cases} |G| & \textit{hvis } \chi = \psi, \\ 0 & \textit{ellers.} \end{cases} \tag{2.15}$$

Bevis. Anta nå at $\chi \neq \chi_0$ er en karakter på G. Da finnes det en $h \in G$ slik at $\chi(h) \neq 1$. Da G er en gruppe, vil hg løpe gjennom G når g gjør det. Setter vi da $S_\chi = \sum_{g \in G} \chi(g)$, har vi

$$\chi(h) S_\chi = \chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g) = S_\chi.$$

Vi valgte h slik at $\chi(h) \neq 1$, og det følger da at $S_\chi = 0$. Så

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{hvis } \chi = \chi_0 \\ 0 & \text{ellers,} \end{cases}$$

og det at $\overline{\chi}\chi(g) = \chi_0(g)$ avslutter beviset. □

Denne ortogonalitetsrelasjonen gir oss et nyttig resultat om de additive karakterene vi har jobbet med tidligere.

Korollar 15. *For vilkårlige heltall m, n, q har vi*

$$\sum_{a=1}^{q} e(an/q)e(-am/q) = \begin{cases} q & \text{hvis } m \equiv n \,(mod\, q) \\ 0 & \text{ellers.} \end{cases} \tag{2.16}$$

Bevis. Vi legger merke til at funksjonen $\chi_{n,q}(a)$ som sender $a \mapsto e(a\frac{n}{q})$ vil være en funksjon slik at $a+b \mapsto e((a+b)\frac{n}{q}) = e(a\frac{n}{q})e(b\frac{n}{q})$. For $a, b \in \mathbb{Z}/q\mathbb{Z}$ vil dette da være en additiv karakter på $\mathbb{Z}/q\mathbb{Z}$. Vi kan da skrive

$$\sum_{a=1}^{q} e(an/q)e(-am/q) = \sum_{a=1}^{q} \chi_{n,q}(a)\overline{\chi}_{m,q}(a),$$

hvor $\chi_{n,q}$ er samme karakter som $\chi_{m,q}$ hvis og bare hvis $m \equiv n \,(mod\, q)$, og resultatet følger da av lemma 14. □

Når vi beviste den første ortogonalitetsrelasjonen summerte vi over $g \in G$ og holdt $\chi \in \hat{G}$ fast. For å bevise den andre ortogonalitetsrelasjonen vil vi la $g \in G$ være fast, og heller la χ løpe gjennom $\hat{G}$. Før vi kan gå igang med det, trenger vi et lite resultat.

Proposisjon 16. *La G være en endelig abelsk gruppe og la $g \neq 1$ være et element i G. Da finnes det en karakter $\chi \in \hat{G}$ med $\chi(g) \neq 1$.*

Bevis. La $g_1, \ldots, g_k$ være et system av uavhenginge generatorer for G slik at hver $g \in G$ har en unik representasjon på samme form som i (2.14). Da g ikke er identitetselementet i G, vil minst en av e_i-ene være slik at $0 < e_i < n_i$. Vi fikserer så en slik i, og lar χ være karakteren på G definert ved $\chi(g_1^{e_1} \cdots g_k^{e_k}) = \eta_i^{e_i}$, hvor η_i er en bestemt n_i-te enhetsrot. Dette vil da være et slikt element vi er ute etter, og vi har $\chi(g) \neq 1$. □

Lemma 17 (Andre ortogonalitetsrelasjon)**.** *La G være en endelig abelsk gruppe og la g, h være to elementer i G. Da har vi*

$$\sum_{\chi \in \hat{G}} \overline{\chi}(g)\chi(h) = \begin{cases} |G| & \text{hvis } g = h, \\ 0 & \text{ellers.} \end{cases} \tag{2.17}$$

Bevis. La $g \neq 1$ være et element i G og velg $\psi \in \hat{G}$ slik at $\psi(g) \neq 1$. Vi setter $S_g = \sum_{\chi \in \hat{G}} \chi(g)$ og da $\hat{G}$ er en gruppe, vil $\psi\chi$ løpe gjennom $\hat{G}$ når χ gjør det. Vi gjør her samme triks som tidligere og har

$$\psi(g)S_g = \psi(g) \sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi \in \hat{G}} (\psi\chi)(g) = \sum_{\chi \in \hat{G}} \chi(g) = S_g.$$

Som gir oss

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} |G| & \text{hvis } g = 1. \\ 0 & \text{ellers} \end{cases}$$

Kombinerer vi nå dette med at

$$\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)} = \overline{\chi}(g),$$

har vi den andre ortogonaltetsrelasjonen. □

Vi er nå klare til å innføre de multiplikative funksjonene som håndteres i den multiplikative store såld, nemlig Dirichlet-karakterene.

2.2.2 Dirichlet-karakterer

Dirichlet-karakterer er funksjoner som er sterkt relatert til karakterene på en endelig abelsk gruppe G. La q være et naturlig tall og la $G = (\mathbb{Z}/q\mathbb{Z})^\star$ være gruppen av enheter modulo q. For hver $\chi \in G$ velger vi oss en tilknyttet funksjon $\tilde{\chi}$ hvor

$$\tilde{\chi}(a) \coloneqq \begin{cases} \chi(a \, mod \, q) & \text{hvis } (a,q) = 1 \\ 0 & \text{ellers} \end{cases}$$

for $a \in \mathbb{Z}$. Denne funksjonen $\tilde{\chi}$ kaller vi en Dirichlet-karakter modulo q. Det at $a + q \equiv a \mod q$ gir oss at $\tilde{\chi}$ er periodisk med periode q. Lar vi $\underline{a}$ være representert av a i $\mathbb{Z}/q\mathbb{Z}$, har vi $\tilde{\chi}(ab) = \chi(\underline{ab}) = \chi(\underline{a})\chi(\underline{b}) = \tilde{\chi}(a)\tilde{\chi}(b)$ for $ab \in \mathbb{Z}$ hvis $(ab, q) = 1$. Skulle derimot $(ab, q) > 1$ vil enten $(a, q) > 1$ eller $(b, q) > 1$, slik at $\tilde{\chi}(ab) = \tilde{\chi}(a)\tilde{\chi}(b) = 0$ og vi har total multiplikativitet for $\tilde{\chi}$. Notasjonsmessig vil vi bruke χ både som funksjonen på G og funksjonen på $\mathbb{Z}$, det vil være klart ut ifra sammenhengen hvilken av disse vi mener. La nå χ være en Dirichlet-karakter modulo q. Da sier vi at d er en kvasiperiode for χ om $\chi(m) = \chi(n)$ hver gang $n \equiv m \mod d$ og $(mn, q) = 1$. Den minste kvasiperioden til χ vil alltid dele q, og vi kaller denne minste kvasiperioden for konduktøren til χ. Om q er konduktøren til χ, kaller vi χ en primitiv karakter. Dette betyr at for en primitiv karakter χ modulo q, så vil det for hver $d|q, d < q$ alltid finnes en a slik at $\chi(a) \neq 1$ hvor $a \equiv 1 \mod d$. Men det finnes også andre måter å se på primitivitet på. Vi sier at en Dirichlet-karakter χ modulo q er indusert av en Dirichlet-karakter χ_i modulo d hvor $d|q$ om

$$\chi(a) = \begin{cases} \chi_i(a) & \text{når } (a,q) = 1 \\ 0 & \text{ellers.} \end{cases}$$

Et annet kriterie for at χ da skal være en primitiv karakter, vil være at χ ikke er indusert av noen Dirichlet-karakterer modulo d hvor, $d \neq q$. Alle Dirichlet-karakterer er enten selv primitive, eller indusert av en primitiv karakter, og vi har for alle $a \in \mathbb{Z}$ at $\chi_i(a) \geq \chi(a)$, hvor χ_i er karakteren som induserer χ. Vi ilustrerer dette ved en tabell over alle Dirichlet-karakterer modulo 15. Gruppen $(\mathbb{Z}/15\mathbb{Z})^*$ er generert av elementene 2 og 11, som har henholdsvis orden 4 og 2.

Dette betyr at $\chi(2)$ kan avbildes på de fjerde enhetsrøttene $\pm 1, \pm i$, mens $\chi(11)$ kan avbildes på ± 1.

$a =$	1	2	4	7	8	11	13	14
$\chi_{0,0}(a)$	1	1	1	1	1	1	1	1
$\chi_{0,1}(a)$	1	1	1	-1	1	-1	-1	-1
$\chi_{1,0}(a)$	1	i	-1	i	$-i$	1	$-i$	-1
$\chi_{1,1}(a)$	1	i	-1	$-i$	$-i$	-1	i	1
$\chi_{2,0}(a)$	1	-1	1	-1	-1	1	-1	1
$\chi_{2,1}(a)$	1	-1	1	1	-1	-1	1	-1
$\chi_{3,0}(a)$	1	$-i$	-1	$-i$	i	1	i	-1
$\chi_{3,1}(a)$	1	$-i$	-1	i	i	-1	$-i$	1

Tabell 2.1: Alle Dirichlet-karakterer modulo 15 hvor, $\chi_{s,t}(a)$ sender $2 \mapsto i^s$ og $11 \mapsto (-1)^t$.

Fra tabellen ser vi at $\chi_{2,1}(a) = 1$ for alle $a \equiv 1 \bmod 3$ (med $(a, 15) = 1$), dette betyr at karakteren ikke er primitiv, og det tar ikke lang tid å sjekke at den blir indusert av karakteren modulo 3 som sender $2 \mapsto -1$. Vi legger også merke til fra tabellen at $\chi_{1,0}, \chi_{2,0}\chi_{3,0}$ alle sender $11 \mapsto 1$, og 11 er det eneste tallet(bortsett fra 1) som er kongruent 1 mod 5. Dette betyr at ingen av disse karakterene heller er primitive, og de eneste primitive Dirichet-karakterene modulo 15 er da $\chi_{0,1}, \chi_{1,1}, \chi_{3,1}$.

Nå som vi har Dirichlet-karakterene på plass, vil vi oversette ortogonalitetsrelasjonene over fra de generelle karakterene.

Proposisjon 18. *La χ være en Dirichlet-karakter modulo q. For $a, b \in \mathbb{Z}$ med $(a, q) = 1$ har vi*

$$\sum_{\chi} \overline{\chi}(a)\chi(b) = \begin{cases} \phi(q) & \textit{hvis } a \equiv b \bmod q, \\ 0 & \textit{ellers.} \end{cases}$$

Hvor summen er over alle Dirichlet-karakterer χ modulo q.

Bevis. Dette følger umiddelbart fra (2.17) om $(a, q) = (b, q) = 1$, og vi velger G til å være $(\mathbb{Z}/q\mathbb{Z})^*$. Skulle derimot $(b, q) > 1$, vil $\chi(b) = 0$. Da $(a, q) = 1$ vet vi at $a \not\equiv b \bmod q$ og vi er i mål. □

Proposisjon 19. *La χ og ψ være to Dirichlet-karakterer modulo q. Da har vi*

$$\sum_{a \,(mod\, q)} \overline{\chi}(a)\psi(a) = \begin{cases} \phi(q) & \textit{hvis } \chi = \psi, \\ 0 & \textit{ellers} \end{cases}$$

Bevis. Igjen la G være $(\mathbb{Z}/q\mathbb{Z})^*$ og dette følger direkte av (2.15). □

Vi innfører nå et verktøy som vil hjelpe oss å koble Dirichlet-karakterene sammen med de additive karakterene.

Definisjon. Gitt en Dirichlet-karakter χ modulo q, da er Gauss-summen

$$\tau(\chi) = \sum_{a \,(mod\, q)} \chi(a) e\Big(\frac{a}{q}\Big).$$

Her er det verdt å merke seg at vi kan legge til betingelsen $(a,q) = 1$ i summen om vi ønsker, for χ forsvinner på de tallene som har en felles faktor med q uansett. Gauss-summen vil være linken mellom den additive og den multiplikative store såld, og før vi kan gå igang med beviset av sistnevnte trenger vi et lemma om den summen.

Lemma 20. *La χ være en primitiv karakter modulo q. Da vil*

(*a*)

$$\tau(\chi)\overline{\chi}(n) = \sum_{a \,(mod\, q)} \chi(a) e\Big(\frac{an}{q}\Big). \tag{2.18}$$

(*b*) $|\tau(\chi)| = \sqrt{q}$.

Bevis. (*a*) Anta først at vi har $(n,q) = 1$. Da er $\{an \,(mod\ q) \,|\, (a,q) = 1\} = \{a \,(mod\ q) \,|\, (a,q) = 1\}$, og vi kan bytte ut a med an i summen. Det betyr at

$$\begin{aligned}
\tau(\chi)\overline{\chi}(n) &= \sum_{a \,(mod\, q)} \chi(an)\overline{\chi}(n) e\Big(\frac{an}{q}\Big) \\
&= \sum_{a \,(mod\, q)} \chi(a)\chi(n)\overline{\chi}(n) e\Big(\frac{an}{q}\Big) \\
&= \sum_{a \,(mod\, q)} \chi(a) e\Big(\frac{an}{q}\Big).
\end{aligned}$$

Anta nå at $(n,q) \neq 1$. Da forsvinner venstresiden i (2.18) fordi χ kun er støttet der $(n,q) = 1$. For å vise at høyresiden forsvinner, hevder vi først at om χ er primitiv, da vil vi for alle $d|q$, $d < q$ og hvert heltall a, ha

$$\sum_{\substack{n=1 \\ n \equiv a \,(mod\, d)}}^{q} \chi(n) = 0. \tag{2.19}$$

Hvis χ er en primitiv karakter modulo q, betyr det at for alle $d|q, d < q$ finnes det m, n slik at $m \equiv n \,(mod\, d)$ og $\chi(m) \neq \chi(n)$ med $\chi(mn) \neq 0$. Da finnes det også en c med $(c,q) = 1$ og $c \equiv 1 \,(mod\, d)$ (velg c til å være inverselementet til m mod q) slik at

$$\begin{aligned}
cm \equiv n \,(mod\, q) \quad &\Rightarrow \quad \chi(c)\chi(m) = \chi(n) \\
&\Rightarrow \quad \chi(c) \neq 1.
\end{aligned}$$

Hvis vi nå har en k som løper gjennom restklassene mod q/d, da vil $n = ac + kcd$ løpe gjennom alle n i restklassene mod q hvor $n \equiv a \bmod d$. Dette betyr at vi

har

$$\sum_{\substack{n=1\\ n\equiv a\,(mod\,d)}}^{q} \chi(n) = \sum_{k=1}^{q/d} \chi(ac+kcd) = \chi(c)\sum_{k=1}^{q/d}\chi(a+kd).$$

Men det å summere $a+kd$ fra $k=1$ til q/d er jo akkurat det samme som å summere alle tall som er kongruent med a mod d over ett løp gjennom restklassene mod q. Så

$$\sum_{\substack{n=1\\ n\equiv a\,(mod\,d)}}^{q} \chi(n) = \chi(c) \sum_{\substack{n=1\\ n\equiv a\,(mod\,d)}}^{q} \chi(n)$$

og da vi har valgt c slik at $\chi(c)\neq 1$ har vi (2.19) . Om nå $(n,q)\neq 1$, lar vi $\frac{m}{d}=\frac{n}{q}$ hvor $(m,d)=1$. Dette impliserer at $d|q$ med $d\neq q$ slik at

$$\sum_{a\,(mod\,q)} \chi(a)e\Big(\frac{an}{q}\Big) = \sum_{h=1}^{d} e\Big(\frac{hm}{d}\Big) \sum_{\substack{a=1\\ a\equiv h\,(mod\,d)}}^{q} \chi(a) = 0,$$

og vi har (a).

(b) Fra (a) vet vi at

$$\begin{aligned}
\phi(q)|\tau(\chi)|^2 &= \sum_{n=1}^{q} \chi(n)\overline{\chi}(n)\tau(\chi)\tau(\overline{\chi}) \\
&= \sum_{n=1}^{q} \sum_{a\,(mod\,q)} \chi(a)e\Big(\frac{an}{q}\Big) \sum_{b\,(mod\,q)} \overline{\chi}(b)e\Big(\frac{-bn}{q}\Big) \\
&= \sum_{a\,(mod\,q)} \sum_{b\,(mod\,q)} \chi(a)\overline{\chi}(b) \sum_{n=1}^{q} e\Big(\frac{(a-b)n}{q}\Big)
\end{aligned}$$

Ligning (2.16) sier oss at den innerste summen her er lik 0 om $a\neq b$, og at summen er lik q om $a=b$. Dette betyr at vi til slutt har

$$\phi(q)|\tau(\chi)|^2 = \sum_{a\,(mod\,q)} |\chi(a)|^2 q = \phi(q)q \Rightarrow |\tau(\chi)| = \sqrt{q}.$$

□

Vi har nå alt vi trenger for å bevise teorem 12, og teoremet vil følge om vi anvender 5 etter litt manipulasjon av Gauss-summer.

Bevis for teorem 12. La $S(\alpha) = \sum_{n=M+1}^{M+N} a_n e(\alpha n)$. Om vi velger en primitiv Dirichet-karakter $\overline{\chi}$ følger det fra (2.18) at

$$\begin{aligned}
\sum_{n=M+1}^{M+N} a_n\chi(n) &= \frac{1}{\tau(\overline{\chi})} \sum_{n=M+1}^{M+N} a_n \sum_{a\,(mod\,q)} \overline{\chi}(a)e\Big(\frac{an}{q}\Big) \\
&= \frac{1}{\tau(\overline{\chi})} \sum_{a\,(mod\,q)} \overline{\chi}(a)S\Big(\frac{a}{q}\Big).
\end{aligned}$$

Kvadrerer vi nå absoluttverdien og ganger med $\frac{q}{\phi(q)}$ på begge sider får vi

$$\frac{q}{\phi(q)}\Big|\sum_{n=M+1}^{M+N} a_n\chi(n)\Big|^2 = \frac{1}{\phi(q)}\Big|\sum_{a\,(mod\,q)}\overline{\chi}(a)S\Big(\frac{a}{q}\Big)\Big|^2,$$

hvor vi har brukt at $|\tau(\chi)|^2 = q$. Summerer vi nå først over $1 \leq q \leq Q$ for så å summere over alle primitive karakterer har vi

$$\frac{1}{\phi(q)}\sum_{q\leq Q}\sideset{}{^\star}\sum_{\chi\,(mod\,q)}\Big|\sum_{a\,(mod\,q)}\overline{\chi}(a)S\Big(\frac{a}{q}\Big)\Big|^2 \leq \frac{1}{\phi(q)}\sum_{q\leq Q}\sideset{}{^\star}\sum_{\chi\,(mod\,q)}1\Big|\sum_{a\,(mod\,q)}S\Big(\frac{a}{q}\Big)\Big|^2.$$

Antallet primitive karakter modulo q er mindre eller lik $\phi(q)$, så vi har her at høyresiden er mindre eller lik

$$\sum_{q\leq Q}\Big|\sum_{a\,(mod\,q)}S\Big(\frac{a}{q}\Big)\Big|^2 = \sum_{q\leq Q}\Big|\sum_{a\,(mod\,q)}\sum_{n=M+1}^{M+N}a_n e\Big(\frac{an}{q}\Big)\Big|^2,$$

og teorem (2.2) gir oss da

$$\sum_{q\leq Q}\Big|\sum_{a\,(mod\,q)}S\Big(\frac{a}{q}\Big)\Big|^2 \leq (Q^2+N-1)\|\vec{a}\|^2.$$

□

2.3 Beviset for Bombieri-Vinogradovs teorem

Nå som vi er ferdige med begge de store såldene, begynner vi å nærme oss et bevis for Bombieri-Vinogradovs teorem. Før vi går videre trenger vi to nye begreper om aritmetiske funksjoner. Teorem 4 omhandler forskjellen mellom en aritmetisk funksjon over en enkelt restklasse, og samme funksjon over gjennomsnittet av restklasser. Følgende differansefunksjon vil derfor være hendig.

Definisjon. La f være en aritmetisk funksjon, da skriver vi

$$D_f(x;q,a) = \sum_{\substack{n\leq x\\ n\equiv a\,(mod\,q)}} f(n) - \frac{1}{\phi(q)}\sum_{\substack{n\leq x\\ (n,q)=1}} f(n).$$

Vi vil også innføre begrepet om Dirichlet-konvulsjoner

Definisjon. Gitt to aritmetiske funksjoner f, g, da er Dirichlet-konvulsjonen

$$(f*g)(n) = \sum_{d|n} f(d)g(n/d).$$

Dirichlet-konvulsjoner er både kommutative og assosiative, noe vi vil ha bruk for senere. Disse konvulsjonenen vil gjøre det lettere å estimere differansefunksjonene vi har definert ovenfor, men det kreves noe arbeid å skrive dem som konvulsjoner. Følgende teorem vil være viktig i beviset av teorem 4.

Teorem 21. *Anta at vi har følger $\alpha = (\alpha_m)$, $\beta = (\beta_n)$ som er støttet på henholdsvis $\{1, \dots M\}$ og $\{1, \dots N\}$. Anta også at*

$$|D_\beta(N; q, a)| \ll \|\vec{\beta}\| N^{\frac{1}{2}} \Delta^9 \text{ for en } \Delta \in (0, 1]. \tag{2.20}$$

La $\gamma = \alpha * \beta$ være Dirichlet-konvulsjonen, da vil

$$\sum_{q \leq Q} \max_{(a,q)=1} |D_\gamma(MN; q, a)| \ll \|\vec{a}\| \|\vec{\beta}\| (\Delta M^{1/2} N^{1/2} + M^{1/2} + N^{1/2} + Q) log^2 Q.$$

Før vi kan gå igang med å bevise dette teoremet, trenger vi noen lemma.

Definisjon. Möbius-funksjonen μ er

$$\mu(n) = \begin{cases} 0 & \text{hvis } p^2 | n \text{ for en } p \in \mathbb{P} \\ (-1)^{\omega(n)} & \text{ellers,} \end{cases}$$

hvor $\omega(n)$ er antallet distinkte primfaktorer av n.

En viktig identitet tilhørende Möbius-funksjon er

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 0 \end{cases}. \tag{2.21}$$

Et bevis for denne kan finnes i [Aub87, ligning 19]. Om $\epsilon(n) = 1$ for $n = 1$ og 0 ellers, mens $I(n)$ er den konstante funksjonen 1 gir denne identiteten oss at $\epsilon(n) = (\mu * I)(n)$. Dette kan vi igjen bruke til å vise en annen viktig egenskap hos Möbius-funksjonen.

Lemma 22 (Möbius inversjonsformel)**.** *Hvis f, og F er to aritmetiske funksjoner slik at*

$$F(n) = \sum_{d|n} f(d)$$

da vil

$$f(n) = \sum_{d|n} \mu(d) F(n/d)$$

Bevis. Ved Dirichlet-konvulsjon har vi

$$f(n) = f * \epsilon = f * (I * \mu) = (f * I) * \mu = F * \mu = \mu * F = \sum_{d|n} \mu(d) F(n/d).$$

□

Möbius-funksjonen og ligning (2.21) bruker vi også for følgende lemma.

Lemma 23. *La $\beta = (\beta_n)$ være støttet på $\{1, \dots N\}$, og la χ være en Dirichlet-karakter modulo q. Da har vi for alle naturlige tall K og s*

$$\sum_{\substack{d|s \\ d\leq K}} \mu(d) \sum_{n\equiv 0 \,(mod\, d)} \beta_n \chi(n) = \sum_{\substack{d|s \\ d\leq K}} \mu(d) \sum_{l|d} \mu(l) \sum_{(n,l)=1} \beta_n \chi(n). \tag{2.22}$$

Bevis. Av lineæritet på β har vi at om dette holder for

$$\beta_n = \begin{cases} 1 & n = n_0 \\ 0 & \text{ellers,} \end{cases} \tag{2.23}$$

så holder det for alle β_n. For en β_n på denne formen blir venstresiden i (2.22)

$$\sum_{\substack{d|s \\ d\leq K}} \mu(d)\chi(n_0) \begin{cases} 1 & d|n_0, (n_0, q) = 1 \\ 0 & \text{ellers} \end{cases}, \tag{2.24}$$

mens høyresiden blir

$$\sum_{\substack{d|s \\ d\leq K}} \mu(d) \sum_{l|d} \mu(l)\chi(n_0) \left\{ \begin{cases} 1 & (n_0, l) = (n_0, q) = 1 \\ 0 & \text{ellers} \end{cases} \right\} = \sum_{\substack{d|s \\ d\leq K \\ (n_0,q)=1}} \mu(d)\chi(n_0) \sum_{\substack{l|d \\ (n_0,l)=1}} \mu(l).$$

Da $\mu(d)$ bare er støttet på kvadratfrie tall, vil den indre summen her være

$$\sum_{\substack{l \,|\, \prod p_i \\ p_i|d \\ (n_0,p_i)=1}} \mu(l),$$

og fra (2.21) har vi at dette er

$$\begin{cases} 1 & \displaystyle\prod_{\substack{p_i|d \\ (n_0,p_i)=1}} p_i = 1 \\ 0 & \text{ellers.} \end{cases}$$

Dette betyr at det ikke er noe bidrag fra de primtallene som deler d og er innbyrdisk primsk med n_0. Det eneste bidraget vi da får er fra det tomme produktet, hvor alle p_i som deler d også har en felles faktor med n_0, altså deler de også n_0. Dette betyr at d deler n_0 og vi ender opp med

$$\sum_{\substack{d|s \\ d\leq K \\ (n_0,q)=1}} \mu(d)\chi(n_0) \begin{cases} 1 & d|n_0 \\ 0 & \text{ellers} \end{cases},$$

som er det samme vi hadde i (2.24). □

Vi vil nå vise at om vi har en følge som tilfredsstiller (2.20), så får man en begrensning på en viss sum som involverer følgen og karakterer.

Lemma 24. *Anta at $\beta = (\beta_n)$ er en følge støttet på $\{1, \dots, N\}$ som tilfredsstiller betingelsen i (2.20). Da vil vi for alle ikke-trivielle karakterer χ modulo r, og naturlige tall s ha*

$$\Big| \sum_{(n,s)=1} \beta_n \chi(n) \Big| \ll \|\vec{\beta}\| N^{1/2} \Delta^3 r \tau(s). \tag{2.25}$$

Bevis. Bruker vi (2.21) har vi

$$\sum_{(n,s)=1} \beta_n \chi(n) = \sum_n \beta_n \chi(n) \sum_{d|(n,s)} \mu(d) = \sum_{d|s} \mu(d) \sum_{n \equiv 0 \,(mod\, d)} \beta_n \chi(n).$$

Vi vil nå dele opp summen i to deler. En del der $d \leq K$, og en del der $d > K$. For delen der $d \leq K$ har vi fra lemma 23 at

$$\sum_{\substack{d|s \\ d \leq K}} \sum_{n \equiv 0 \,(mod\, d)} \beta_n \chi(n) = \sum_{\substack{d|s \\ d \leq K}} \mu(d) \sum_{l|d} \mu(l) \sum_{(n,l)=1} \beta_n \chi(n).$$

Ser vi nå på den indre summen over restklassene mod lr hvor $(l, r) = 1$ kan vi skrive

$$\begin{aligned}
\sum_{(n,l)=1} \beta_n \chi(n) &= \sum_{\substack{a=1 \\ (a,lr)=1}}^{lr} \sum_{\substack{n \equiv a \,(mod\, lr) \\ n \leq N}} \beta_n \chi(n) \\
&= \sum_{\substack{a=1 \\ (a,lr)=1}}^{lr} \chi(a) \sum_{\substack{n \equiv a \,(mod\, lr) \\ n \leq N}} \beta_n \\
&= \sum_{\substack{a=1 \\ (a,lr)=1}}^{lr} \chi(a) \Big(D_\beta(N; lr, a) + \frac{1}{\phi(lr)} \sum_{\substack{(n,lr)=1 \\ n \leq N}} \beta_n \Big) \\
&= \frac{1}{\phi(lr)} \sum_{\substack{a=1 \\ (a,lr)=1}}^{lr} \chi(a) \sum_{\substack{(n,lr)=1 \\ n \leq N}} \beta_n + \sum_{\substack{a=1 \\ (a,lr)=1}}^{lr} \chi(a) D_\beta(N; lr, a).
\end{aligned}$$

Her vil den første summen forsvinne da

$$\sum_{\substack{a=1 \\ (a,lr)=1}}^{lr} \chi(a) = 0,$$

og β_n ikke avhenger av a. Videre har vi at

$$\begin{aligned}
\Big| \sum_{\substack{a=1 \\ (a,lr)=1}}^{lr} \chi(a) D_\beta(N; lr, a) \Big| &\leq \sum_{\substack{a=1 \\ (a,lr)=1}}^{lr} \big|\chi(a)\big| \big|D_\beta(N; lr, a)\big| \\
&\ll \phi(lr) \|\vec{\beta}\| N^{1/2} \Delta^9,
\end{aligned}$$

fra antagelsen om at (2.20) holder for β. Vi har da at summen vår over $d \leq K$ er

$$\ll \|\vec{\beta}\| N^{1/2} \Delta^9 \sum_{\substack{d|s \\ d \leq K}} |\mu(d)| \sum_{l|d} |\mu(l)| \phi(lr) \leq \|\vec{\beta}\| N^{1/2} \Delta^9 K \phi(r) \tau(s),$$

hvor vi har brukt at

$$\phi(lr) = \phi(l)\phi(r)$$

for $(l, r) = 1$, samt at

$$\sum_{l|d} \phi(l) = d \leq K \text{ og } \sum_{\substack{d|s \\ d \leq K}} 1 \leq \tau(s).$$

Vi vil for delen der $d > K$ ha

$$\sum_{\substack{d|s \\ d > K}} \mu(d) \sum_{n \equiv 0 \, (mod \, d)} \beta_n \chi(n).$$

Om vi nå bruker Cauchy–Schwarz' ulikhet på den indre summen, har vi

$$\begin{aligned} \left| \sum_{n \equiv 0 \, (mod \, d)} \beta_n \chi(n) \right|^2 &\leq \sum_{n \equiv 0 (mod \, d)} |\beta_n|^2 \sum_{n \equiv 0 \, (mod \, d)} |(\chi(n))|^2 \\ &\leq \|\vec{\beta}\|^2 \frac{N}{d}. \end{aligned}$$

Slik at summasjonen over $d > K$ gir oss

$$\|\vec{\beta}\| N^{1/2} \sum_{\substack{d|s \\ d > K}} d^{-1/2} \leq \|\vec{\beta}\| N^{1/2} K^{-1/2} \tau(s).$$

Det kan ikke være mer enn $\tau(s)$ slike d-er, og for hver av d-ene vil

$$d^{-1/2} < K^{-1/2}.$$

Setter vi nå til slutt $K = \Delta^{-6}$ får vi

$$\begin{aligned} \left| \sum_{(n,s)=1} \beta_n \chi(n) \right| &\ll \|\vec{\beta}\| N^{1/2} \Delta^3 \phi(r) \tau(s) + \|\vec{\beta}\| N^{1/2} \Delta^3 \tau(s) \\ &\leq \|\vec{\beta}\| N^{1/2} \Delta^3 r \tau(s). \end{aligned}$$

□

Det neste vi trenger er et lemma som gjør det mulig å skrive $D_\gamma(MN; q, a)$ som et produkt av summer, istedenfor å være en differanse. Det vil gjøre det lettere å begrense $\max |D_\gamma(MN; q, a)|$ om vi har det på en slik form.

Lemma 25.

$$D_\gamma(MN;q,a)=\frac{1}{\phi(q)}\sum_{\substack{\chi\,(mod\,q)\\ \chi\neq\chi_0}}\overline{\chi}(a)\Big(\sum_{m\leq M}\alpha_m\chi(m)\Big)\Big(\sum_{n\leq N}\beta_n\chi(n)\Big) \tag{2.26}$$

hvor $\gamma=\alpha*\beta$.

Bevis. Fra definisjonen har vi

$$D_\gamma(MN;q,a)=\sum_{\substack{k\leq MN\\ k\equiv a\,(mod\,q)}}\gamma(k)-\frac{1}{\phi(q)}\sum_{\substack{k\leq MN\\ (k,q)=1}}\gamma(k).$$

Ortogonalitet gjør at vi kan erstatte betingelsen $k\equiv a\,(mod\,q)$ med summen

$$\frac{1}{\phi(q)}\sum_{\chi\,(mod\,q)}\chi(k)\overline{\chi}(a),$$

som gir oss

$$\frac{1}{\phi(q)}\sum_{\substack{k\leq MN\\ (k,q)=1}}\sum_{\chi\,(mod\,q)}\chi(k)\overline{\chi}(a)\gamma(k)-\frac{1}{\phi(q)}\sum_{\substack{k\leq MN\\ (k,q)=1}}\gamma(k). \tag{2.27}$$

For den trivielle karakteren vil

$$\sum_{\substack{k\leq MN\\ (k,q)=1}}\chi_0(k)\gamma(k)=\sum_{\substack{k\leq MN\\ (k,q)=1}}\gamma(k),$$

som kanselererer det siste leddet i (2.27) slik at vi står igjen med

$$\frac{1}{\phi(q)}\sum_{\substack{k\leq MN\\ (k,q)=1}}\sum_{\chi\neq\chi_0\,(mod\,q)}\overline{\chi}(a)\chi(k)\gamma(k)=\frac{1}{\phi(q)}\sum_{\chi\neq\chi_0\,(mod\,q)}\overline{\chi}(a)\sum_{\substack{k\leq MN\\ (k,q)=1}}\chi(k)\gamma(k).$$

Det eneste som nå står igjen å vise, er at

$$\sum_{\substack{k\leq MN\\ (k,q)=1}}\chi(k)\gamma(k)=\Big(\sum_{m\leq M}\alpha_m\chi(m)\Big)\Big(\sum_{n\leq N}\beta_n\chi(n)\Big).$$

Vi begynner med

$$\Big(\sum_{m\leq M}\alpha_m\chi(m)\Big)\Big(\sum_{n\leq N}\beta_n\chi(n)\Big)=\sum_{m\leq M}\sum_{n\leq N}\alpha_m\beta_n\chi(mn),$$

og setter vi nå $k=mn$ vil koeffisientene foran $\chi(k)$ være summen av alle $\alpha_m\beta_n$ med $mn=k$. Dette vil være Dirichlet-konvulsjonen $\sum_{mn=k}\alpha(m)\beta(n)=\gamma(k)$ og det faller rett ut at

$$\sum_{m\leq M}\sum_{n\leq N}\alpha_m\beta_n\chi(mn)=\sum_{\substack{k\leq MN\\ (k,q)=1}}\chi(k)\gamma(k).$$

□

Før vi går videre tar vi med oss to resultater om summer som vi vil ha bruk for senere.

Lemma 26. (*a*)

$$\sum_{s\leq Q}\frac{\tau(s)}{\phi(s)}\ll \log^2 Q. \tag{2.28}$$

(*b*)

$$\sum_{s\leq Q}\frac{1}{\phi(s)}\ll \log Q. \tag{2.29}$$

Bevis. (*a*) Først hevder vi ganske uskyldig at vi for alle ikke negative multiplikative funksjoner $f(n)$ har

$$\sum_{n\leq x} f(n)\leq \prod_{p\leq x}\sum_{k=0}^{\infty} f(p^k). \tag{2.30}$$

Lar vi

$$n=\prod p^{a_p}$$

være primtallsfaktoriseringen av n, vil $p\leq x$ for alle p da $p\leq n$, og alle produkter av disse p^{a_p} vil forekomme på høyresiden av ulikheten. Bruker vi

$$f(n)=\prod f(p^{a_p})$$

får vi (2.30). Både $\tau(s)$ og $\phi(s)$ er ikke negative multiplikative funksjoner, og $\phi(s)>0$ for alle s, så det er klart at (2.30) også holder for $\dfrac{\tau(s)}{\phi(s)}$. Da har vi

$$\sum_{s\leq Q}\frac{\tau(s)}{\phi(s)}\leq \prod_{p\leq Q}\sum_{k=0}^{\infty}\frac{\tau(p^k)}{\phi(p^k)},$$

og bruker vi nå at $\tau(p^k)=k+1$ og $\phi(p^k)=p^{k-1}(p-1)$, får vi

$$\sum_{s\leq Q}\frac{\tau(s)}{\phi(s)}\leq \prod_{p\leq Q}\left(1+\sum_{k=1}^{\infty}\frac{k+1}{p^{k-1}(p-1)}\right).$$

Denne summen er absolutt konvergent for enhver p, så vi har lov til å forandre summasjonen slik at

$$1+\sum_{k=1}^{\infty}\frac{k+1}{p^{k-1}(p-1)}=\left(1+\sum_{k=1}^{\infty}\frac{1}{p^{k-1}(p-1)}\right)+\sum_{l=1}^{\infty}\sum_{k=l}^{\infty}\frac{1}{p^{k-1}(p-1)}.$$

Dette stemmer da hvert ledd vil forekomme èn gang i den første summen, og k ganger i den doble summen, én gang for hver $1\leq l\leq k$. Summen av en

geometriske rekke gir oss at dette er

$$\begin{aligned} 1+\frac{1}{p-1}\frac{1}{1-\frac{1}{p}} &+ \sum_{l=1}^{\infty}\frac{1}{p^{l-1}(p-1)}\frac{1}{1-\frac{1}{p}} \\ &= 1+\frac{p}{(p-1)^2}+\frac{1}{(p-1)^2}\sum_{l=1}^{\infty}p^{2-l}, \end{aligned}$$

som igjen gir oss

$$1+\frac{p}{(p-1)^2}+\frac{p^2}{(p-1)^3}=1+\frac{2p^2-p}{(p-1)^3}.$$

Logaritmen til et produkt er produktet av logaritmene, slik at uttrykket vi står igjen med å estimere er

$$\exp\Big(\sum_{p\leq Q}\log\Big(1+\frac{2p^2-p}{(p-1)^3}\Big)\Big).$$

Vi bruker nå at $\log(1+x)\leq x$ slik at

$$\log\Big(1+\frac{2p^2-p}{(p-1)^3}\Big)\leq\frac{2p^2-p}{(p-1)^3}=\frac{2}{p-1}+O\Big(\frac{1}{(p-1)^2}\Big)=\frac{2}{p}+O\Big(\frac{1}{p^2}\Big).$$

Vi minner nå om Mertens første teorem[Pol09, teorem 3.14] som sier at når $x\to\infty$ har vi

$$\sum_{p\leq x}\frac{1}{p}=\log\log x+B_1+O(1/\log x),$$

for en konstant B_1 . Bruker vi nå dette resultatet samtidig som vi tar med oss at $\sum\frac{1}{p^2}\leq\sum\frac{1}{n^2}$ er konverget har vi når $Q\to\infty$ at

$$\begin{aligned} \sum_{s\leq Q}\frac{\tau(s)}{\phi(s)} &\leq \exp\Big(2\log\log Q+2B_1+O(2/\log Q)+C\Big) \\ &= \exp\Big(2\log\log Q+C+O(1/\log Q)\Big) \\ &\leq e^{2\log\log Q}e^C=C\log^2 Q, \end{aligned}$$

hvor vi har samlet sammen konstantene i en felles konstant C. (b) Akkurat som i (a) kan vi få

$$\begin{aligned} \sum_{s\leq Q}\frac{1}{\phi(s)} &\leq \prod_{p\leq Q}\sum_{k=0}^{\infty}\frac{1}{\phi(p^k)} \\ &= \prod_{p\leq Q}\Big(1+\sum_{k=1}^{\infty}\frac{1}{p^{k-1}(p-1)}\Big) \\ &= \prod_{p\leq Q}\Big(1+\frac{p}{(p-1)^2}\Big). \end{aligned}$$

Gjør nå igjen det samme trikset med å summere over logaritmene, slik at

$$\begin{aligned}\sum_{s\le Q}\frac{1}{\phi(s)} &\le \exp\Big(\sum_{p\le Q}\log\Big(1+\frac{p}{(p-1)^2}\Big)\Big)\\ &\le \exp\Big(\sum_{p\le Q}\frac{p}{(p-1)^2}\Big)\\ &= \exp\Big(\sum_{p\le Q}\frac{1}{p}+O\Big(\sum_{p\le Q}\frac{1}{(p-1)^2}\Big)\Big)\\ &\ll \log Q.\end{aligned}$$

□

Vi er nå klare for å bevise teorem 21. Vi har lyst til å bruke lemma 25, men istedenfor å summere over alle karakterer vil vi heller summere over primitive karakterer, og dermed kunne anvende den multiplikative store såld. Vi kommer også til å dele intervallet fra 1 til Q opp i mindre deler, hvor det vil være lønnsomt å konsentrere seg om delene hver for seg.

Bevis. Fra lemma 25 har vi

$$D_\gamma(MN;q,a)=\frac{1}{\phi(q)}\sum_{\substack{\chi(\bmod q)\\ \chi\neq\chi_0}}\overline{\chi}(a)\Big(\sum_m\alpha_m\chi(m)\Big)\Big(\sum_n\beta_n\chi(n)\Big),$$

men vi ønsker istedet å summere over primitive karakterer. Alle karakterer er primitive eller indusert av en primitiv karakter, slik at vi får en øvre begrensning om vi summerer over alle primitive Dirichlet-karakterer modulo r, for alle $r\le q$. Om χ er indusert av en primitiv karakter modulo r, vil r dele q slik at det finnes s hvor $q=rs$. Bruker vi at $\phi(q)\ge\phi(r)\phi(s)$ har vi

$$\sum_{q\le Q}\max_{(a,q)=1}|D_\gamma(MN;q,a)|$$

$$= \sum_{q\le Q}\max_{(a,q)=1}\Big|\frac{1}{\phi(q)}\sum_{\substack{\chi\,(\mathrm{mod}\,q)\\ \chi\neq\chi_0}}\overline{\chi}(a)\Big(\sum_m \alpha_m\chi(m)\Big)\Big(\sum_n \beta_n\chi(n)\Big)\Big|$$

$$\le \sum_{s\le Q}\frac{1}{\phi(s)}\sum_{1<r\le Q}\frac{1}{\phi(r)}\sideset{}{^\star}\sum_{\chi\,(\mathrm{mod}\,r)}\Big|\sum_{(m,s)=1}\alpha_m\chi(m)\Big|\Big|\sum_{(n,s)=1}\beta_n\chi(n)\Big|,$$

hvor $\sum^\star$ betyr at vi summerer over primitve karakterer og vi har brukt at $r\neq 1$ da $\chi\neq\chi_0$. Vi vil nå separere summen for forskjellig verdier av r. For $r\le R$ (R velges senere) kan vi bruke lemma 24 til å få

$$\sum_{s\le Q}\frac{1}{\phi(s)}\sum_{1<r\le R}\frac{1}{\phi(r)}\sideset{}{^\star}\sum_{\chi\,(\mathrm{mod}\,r)}\Big|\sum_{(m,s)=1}\alpha_m\chi(m)\Big|\Big|\sum_{(n,s)=1}\beta_n\chi(n)\Big|$$

$$\le \|\vec{\beta}\|N^{1/2}\Delta^3\sum_{s\le Q}\frac{\tau(s)}{\phi(s)}\sum_{1<r\le R}\frac{r}{\phi(r)}\sideset{}{^\star}\sum_{\chi\,(\mathrm{mod}\,r)}\Big|\sum_{(m,s)=1}\alpha_m\chi(m)\Big|.$$

Sammen med

$$\Big|\sum_{(m,s)=1}\alpha_m\chi(m)\Big|\le\Big(\sum_{(m,s)=1}|\alpha_m\chi(m)|^2\Big)^{1/2}\le\|\vec{\alpha}\|,$$

bruker vi (2.28) slik at summen vår for $r\le R$ da vil være

$$\ll\|\vec{\alpha}\|\|\vec{\beta}\|N^{1/2}\Delta^3\sum_{s\le Q}\frac{\tau(s)}{\phi(s)}\sum_{1<r\le R}r\ll\|\vec{\alpha}\|\|\vec{\beta}\|N^{1/2}\Delta^3R^2\log^2Q.$$

For verdier $R<r\le Q$ kommer vi til å sepparere summene inn i intervaller $\{P+1,\dots 2P\}$, hvor $P=R,2R,4R,\dots$, som maksimalt gir oss $O(\log Q)$ slike intervaller. Over disse intervallene får vi da

$$\sum_{s\le Q}\frac{1}{\phi(s)}\sum_{P<r\le 2P}\frac{1}{\phi(r)}\sideset{}{^\star}\sum_{\chi\,(\mathrm{mod}\,r)}\Big|\sum_{(m,s)=1}\alpha_m\chi(m)\Big|\Big|\sum_{(n,s)=1}\beta_n\chi(n)\Big|.$$

Cauchy–Schwarz' ulikhet gir oss

$$\sideset{}{^\star}\sum_{\chi\,(\mathrm{mod}\,r)}\Big|\sum_{(m,s)=1}\alpha_m\chi(m)\Big|\Big|\sum_{(n,s)=1}\beta_n\chi(n)\Big|$$

$$\le\Big(\sideset{}{^\star}\sum_{\chi\,(\mathrm{mod}\,r)}\Big|\sum_{(m,s)=1}\alpha_m\chi(m)\Big|^2\Big)^{1/2}\Big(\sideset{}{^\star}\sum_{\chi\,(\mathrm{mod}\,r)}\Big|\sum_{(n,s)=1}\beta_n\chi(n)\Big|^2\Big)^{1/2},$$

så fra teorem 12 (hvor det for oss holder å bruke Q^2+N) får vi

$$\sum_{P<r\leq 2P}\frac{1}{\phi(r)}\sideset{}{^\star}\sum_{\chi\,(mod\,r)}\left|\sum_{(m,s)=1}\alpha_m\chi(m)\right|\left|\sum_{(n,s)=1}\beta_n\chi(n)\right|$$

$$\begin{aligned}
&\leq \frac{1}{P}\sum_{P<r\leq 2P}\frac{r^2}{(\phi(r))^2}\sideset{}{^\star}\sum_{\chi\,(mod\,r)}\left|\sum_{(m,s)=1}\alpha_m\chi(m)\right|\left|\sum_{(n,s)=1}\beta_n\chi(n)\right|\\
&\leq \frac{1}{P}(P^2+M)^{1/2}(P^2+N)^{1/2}\|\vec{\alpha}\|\|\vec{\beta}\|\\
&\leq \frac{1}{P}(P+M^{1/2})(P+N)^{1/2}\|\vec{\alpha}\|\|\vec{\beta}\|\\
&\ll \|\vec{\alpha}\|\|\vec{\beta}\|(P+M^{1/2}+N^{1/2}+P^{-1}M^{1/2}N^{1/2}),
\end{aligned}$$

hvor vi har brukt at $\sqrt{a+b}\leq\sqrt{a}+\sqrt{b}$. Det at $R\leq P\leq Q$, sammen med (2.29) og det faktum at det er maksimalt $O(\log Q)$ slike summer gir oss at summen for $r>R$ er

$$\ll \|\vec{a}\|\|\vec{\beta}\|(Q+M^{1/2}+N^{1/2}+R^{-1}M^{1/2}N^{1/2})(\log^2 Q).$$

Velger vi $R=\Delta^{-1}$ ser vi at dette bidraget vil være større enn bidraget for $r\leq R$ og derfor være det gjelende. □

Vi er nå klare for å gå igang med den siste delen av beviset for 4.

Vi har lyst til å kunne bruke teorem 21 direkte på Λ, men dette kan vi ikke gjøre på grunn av betingelsen $n\leq x$. Vi er derfor nødt til å dele Λ opp i forskjellige biter. På noen biter vil vi kunne anvende teorem 21, mens andre biter må estimeres ved hjelp av andre teknikker. Det første vi nå gjør er å gjengi en identitet for Von Mangoldt-funksjonen kalt Vaughans identiet, et bevis for den kan man finne i [IK04, prop 13.4].

$$\Lambda(n)=\sum_{\substack{m\leq y\\ m|n}}\mu(m)\log\left(\frac{n}{m}\right)-\sum_{\substack{m\leq y\\ k\leq z\\ km|n}}\mu(m)\Lambda(k)+\sum_{\substack{m>y\\ k>z\\ km|n}}\mu(m)\Lambda(k). \tag{2.31}$$

Vi trenger også en tilhørende funksjon som vil hjelpe oss med å utrykke Λ som en konvulsjon, nemlig den ufullstendige logaritmen

$$\lambda(l,x)=\log l-\sum_{\substack{k\leq x^{1/5}\\ k|l}}\Lambda(k).$$

Notasjonsmessig vil vi som regel utelate x fra argumentet og bare skrive $\lambda(l)$. Ved hjelp av (2.31) deler vi nå Λ opp i biter som begynner å ligne konvulsjoner av λ og μ hvor vi etterhvert kan anvende teorem21.

Lemma 27. *Om $x^{1/5} < n \le x$, har vi*

$$\Lambda(n) = \sum_{\substack{m \le x^{1/5} \\ lm = n}} \lambda(l)\mu(m) + \sum_{\substack{x^{1/5} < m \le x^{4/5} \\ lm = n}} \lambda(l)\mu(m). \tag{2.32}$$

Bevis. Setter inn for $\lambda(l)$ slik at

$$\sum_{\substack{m \le x^{1/5} \\ lm = n}} \lambda(l)\mu(m) + \sum_{\substack{x^{1/5} < m \le x^{4/5} \\ lm = n}} \lambda(l)\mu(m)$$

$$= \sum_{\substack{m \le x^{1/5} \\ lm = n}} \Big(\log l - \sum_{\substack{k \le x^{1/5} \\ k \mid l}} \Lambda(k) \Big) \mu(m) + \sum_{\substack{x^{1/5} < m \le x^{4/5} \\ lm = n}} \Big(\log l - \sum_{\substack{k \le x^{1/5} \\ k \mid l}} \Lambda(k) \Big) \mu(m)$$

$$= \sum_{\substack{m \le x^{1/5} \\ m \mid n}} \mu(m) \log\Big(\frac{n}{m}\Big) - \sum_{\substack{m \le x^{1/5} \\ lm = n}} \sum_{\substack{k \le x^{1/5} \\ k \mid l}} \Lambda(k)\mu(m)$$

$$+ \sum_{\substack{x^{1/5} < m \le x^{4/5} \\ lm = n}} \Big(\log l - \sum_{\substack{k \le x^{1/5} \\ k \mid l}} \Lambda(k \Big) \mu(m).$$

I de summene hvor vi nå har både $lm = n$ og $k|l$, setter vi istedet inn betingelsen $km|n$ slik at vi får

$$\sum_{\substack{m \le x^{1/5} \\ m \mid n}} \mu(m) \log\Big(\frac{n}{m}\Big) - \sum_{\substack{m \le x^{1/5} \\ k \le x^{1/5} \\ km \mid n}} \mu(m)\Lambda(k)$$

$$+ \sum_{\substack{x^{1/5} < m \le x^{4/5} \\ lm = n}} \mu(m) \log l - \sum_{\substack{x^{1/5} < m \le x^{4/5} \\ k \le x^{1/5} \\ km \mid n}} \Lambda(k)\mu(m).$$

Bruker vi nå at $\log l = \sum_{k|l} \Lambda(k)$ har vi for de to siste summene her

$$\sum_{\substack{x^{1/5} < m \le x^{4/5} \\ lm = n}} \mu(m) \log l - \sum_{\substack{x^{1/5} < m \le x^{4/5} \\ k \le x^{1/5} \\ km \mid n}} \Lambda(k)\mu(m)$$

$$= \sum_{\substack{x^{1/5} < m \le x^{4/5} \\ lm = n}} \mu(m) \sum_{k \mid l} \Lambda(k) - \sum_{\substack{x^{1/5} < m \le x^{4/5} \\ k \le x^{1/5} \\ km \mid n}} \Lambda(k)\mu(m)$$

$$= \sum_{\substack{x^{1/5} < m \le x^{4/5} \\ km \mid n}} \mu(m)\Lambda(k) - \sum_{\substack{x^{1/5} < m \le x^{4/5} \\ k \le x^{1/5} \\ km \mid n}} \mu(m)\Lambda(k) = \sum_{\substack{x^{1/5} < m \le x^{4/5} \\ k > x^{1/5} \\ km \mid n}} \mu(m)\Lambda(k).$$

Her ser vi at vi kan forenkle betingelsen $x^{1/5} < m \leq x^{4/5}$ til $x^{1/5} < m$ da vi for $m > x^{4/5}, k > x^{1/5}$ har $km > x \geq n$ slik at km ikke kan dele n. Slår vi nå sammen summene står vi igjen med

$$\sum_{\substack{m \leq x^{1/5} \\ lm=n}} \lambda(l)\mu(m) + \sum_{\substack{x^{1/5} < m \leq x^{4/5} \\ lm=n}} \lambda(l)\mu(m)$$
$$= \sum_{\substack{m \leq x^{1/5} \\ m|n}} \mu(m) \log\left(\frac{n}{m}\right) - \sum_{\substack{m \leq x^{1/5} \\ k \leq x^{1/5} \\ km|n}} \mu(m)\Lambda(k) + \sum_{\substack{m > x^{1/5} \\ k > x^{1/5} \\ km|n}} \mu(m)\Lambda(k).$$

Om vi nå bruker $y = z = x^{1/5}$ ser vi at dette er på samme form som i (2.31) og vi er i mål. □

Vi navngir nå summene

$$\Lambda^\sharp(n) = \sum_{\substack{m \leq x^{1/5} \\ lm=n}} \lambda(l)\mu(m)$$

og

$$\Lambda^\flat(n) = \sum_{\substack{x^{1/5} < m \leq x^{4/5} \\ lm=n}} \lambda(l)\mu(m).$$

For det området hvor (2.32) ikke holder har vi det trivielle estimatet

$$\sum_{\substack{n \leq x^{1/5} \\ n \equiv a \,(mod\, q)}} \Lambda(n) - \frac{1}{\phi(q)} \sum_{\substack{n \leq x^{1/5} \\ (n,q)=1}} \Lambda(n) \ll \sum_{n \leq x^{1/5}} \log n \leq x^{1/5} \log x,$$

slik at

$$D_\Lambda(x; q, a) = D_{\Lambda^\sharp}(x; q, a) + D_{\Lambda^\flat}(x; q, a) + O(x^{1/5} \log x). \tag{2.33}$$

Vi vil nå estimere $D_{\Lambda^\sharp}(x; q, a)$ og $D_{\Lambda^\flat}(x; q, a)$ hver for seg, og planen er etterhvert å kunne bruke teorem 21 på sistnevnte.

Lemma 28.

$$\sum_{q \leq Q} \max_{(a,q)=1} |D_{\Lambda^\sharp}(x; q, a)| \ll Qx^{2/5}$$

Bevis. Det første vi vil vise er at om f er en kontinuerlig og positiv monoton funksjon på $[1, y]$, har vi

$$|D_f(y; q, a) \leq |f(1)| + 2|f(y)|. \tag{2.34}$$

Ser da på

$$|D_f(y; q, a)| = \left| \sum_{\substack{n \leq y \\ n \equiv a \,(mod\, q)}} f(n) - \frac{1}{\phi(q)} \sum_{\substack{n \leq y \\ (n,q)=1}} f(n) \right|$$

Det vi nå vil gjøre, er å overestimere de positive leddene, og underestimere de negative leddene. Der $n \equiv a \,(mod\, q)$ kan vi skrive skrive $n = a + kq$ og vi har at $|f(n)| \leq |f((k+1)q)|$, da f er monoton. Der hvor n skal være innbyrdes primsk med q, kan vi skrive $n = a' + kq$, hvor $(a', q) = 1$. I hvert intervall $[kq, (k+1)q)$ vil vi ha $\phi(q)$ slike n-er, hvor vi for alle vil ha $|f(n)| \geq |f(kq)|$. Lar vi nå K være den største K hvor $|f(Kq)| < |f(y)|$ har vi

$$|D_f(y; q, a)| \leq \left| f(y) + \sum_{k=1}^{K} f(kq) - f(1) - \frac{1}{\phi(q)} \sum_{k=2}^{K} \phi(q) f((k-1)q) \right|$$

$$= \left| f(y) + f(Kq) - f(1) \right| \leq 2|f(y)| + |f(1)|.$$

Ser vi nå på $D_\lambda(x; q, a)$ og velger $f(n) = \log(n)$ og $f(n) = 1$ i (2.34) får vi

$$|D_\lambda(x; q, a)|$$

$$= \left| \sum_{\substack{n \equiv a \,(mod\, q) \\ n \leq x}} \left(\log n - \sum_{\substack{k|n \\ k \leq x^{1/5}}} \Lambda(k) \right) - \frac{1}{\phi(q)} \left(\sum_{\substack{(n,q)=1 \\ n \leq x}} \left(\log n - \sum_{\substack{k|n \\ k \leq x^{1/5}}} \Lambda(k) \right) \right) \right|$$

$$\leq \left| \sum_{\substack{n \equiv a \,(mod\, q) \\ n \leq x}} \log n - \frac{1}{\phi(q)} \sum_{\substack{(n,q)=1 \\ n \leq x}} \log n) \right|$$

$$+ \sum_{k \leq x^{1/5}} \Lambda(k) \left| \left(\sum_{\substack{n \equiv a \,(mod\, q) \\ n \equiv 0 \,(mod\, k) \\ n \leq x}} 1 - \frac{1}{\phi(q)} \sum_{\substack{(n,q)=1 \\ n \equiv 0 \,(mod\, k) \\ n \leq x}} 1 \right) \right|$$

hvor vi har brukt at

$$\sum_{\substack{n \leq x \\ n \equiv a \,(mod\, q)}} \sum_{\substack{k \leq x^{1/5} \\ k|n}} \Lambda(k) - \frac{1}{\phi(q)} \sum_{\substack{n \leq x \\ (n,q)=1}} \sum_{\substack{k \leq x^{1/5} \\ k|n}} \Lambda(k)$$

$$= \sum_{k \leq x^{1/5}} \left(\sum_{\substack{n \leq x \\ n \equiv a \,(mod\, q) \\ n \equiv 0 \,(mod\, k)}} 1 - \frac{1}{\phi(q)} \sum_{\substack{n \leq x \\ (n,q)=1 \\ n \equiv 0 \,(mod\, k)}} 1 \right).$$

Dette betyr at vi har

$$|D_\lambda(x; q, a)| \leq 2|\log x| + 3 \sum_{k \leq x^{1/5}} \Lambda(k),$$

og fra Primtallsteoremet vet vi at $\sum_{k \leq x^{1/5}} \Lambda(k) = \psi(x^{1/5}) \ll x^{1/5}$, og da $x^{1/5} + \log x \ll x^{1/5}$ har vi $|D_\lambda(x; q, a)| \ll x^{1/5}$. Vi kan nå manipulere summene slik at vi får

$$\sum_{q\le Q}\max_{(a,q)=1}|D_{\Lambda^\sharp}(x;q,a)|$$

$$\begin{aligned}
&= \sum_{q\le Q}\max_{(a,q)=1}\Bigg|\sum_{\substack{n\le x\\ n\equiv a\,(\mathrm{mod}\,q)}}\sum_{\substack{m\le x^{1/5}\\ m\mid n\\ lm=n}}\lambda(l)\mu(m)-\frac{1}{\phi(q)}\sum_{\substack{n\le x\\ (n,q)=1}}\sum_{\substack{m\le x^{1/5}\\ m\mid n\\ lm=n}}\lambda(l)\mu(m)\Bigg|\\
&= \sum_{q\le Q}\max_{(a,q)=1}\Bigg|\sum_{\substack{m\le x^{1/5}\\ (m,q)=1}}\mu(m)\sum_{\substack{l\le x/m\\ l\equiv am^{-1}\,(\mathrm{mod}\,q)}}\lambda(l)-\frac{1}{\phi(q)}\sum_{\substack{m\le x^{1/5}\\ (m,q)=1}}\mu(m)\sum_{\substack{l\le x/m\\ (l,q)=1}}\lambda(l)\Bigg|\\
&\le \sum_{q\le Q}\sum_{\substack{m\le x^{1/5}\\ (m,q)=1}}|\mu(m)|\max_{(a,q)=1}\Bigg|\sum_{\substack{l\le x/m\\ l\equiv am^{-1}\,(\mathrm{mod}\,q)}}\lambda(l)-\frac{1}{\phi(q)}\sum_{\substack{l\le x/m\\ (l,q)=1}}\lambda(l)\Bigg|\\
&\ll \sum_{q\le Q}\sum_{\substack{m\le x^{1/5}\\ (m,q)=1}}|\mu(m)|x^{1/5}\ll Qx^{2/5},
\end{aligned}$$

hvor vi har brukt at $x^{1/5}m^{-1/5}\ll x^{1/5}$. □

Vi trenger nå et estimat for $D_{\Lambda^\flat}(x;q,a)$, og vi ønsker å kunne bruke teorem 21. For å gjøre dette er vi nødt til å kunne skrive $\Lambda^\flat(n)$ som en konvulsjon av to funksjoner. Det har vi nesten, bortsett fra at betingelsen $lm=n\le x$ gjør at l og m er sammenkoblet. For å få til å kunne skrive det som en konvulsjon, deler vi intervallet vårt fra 1 til x opp i intervaller $[(1+\delta)^j,(1+\delta)^{j+1})$. Det vil være $O(\delta^{-1}\log x)$ slike intervaller. For om vi kaller antallet intervaller J, har vi

$$(1+\delta)^J\le x\implies J\log(1+\delta)\le\log x$$

så

$$J\le\frac{\log x}{\log(1+\delta)}\ll\delta^{-1}\log x.$$

Vi vil da også forandre summasjonsbetingelsene fra $lm=n$, $x^{1/5}<m\le x^{4/5}$, til $lm=n$, $L<l<(1+\delta)L$, $M<m<(1+\delta)M$, hvor L,M er på formen $(1+\delta)^j$, og $L>x^{1/5}$, $M<x^{4/5}$, $LM<x$. Denne dekningen vil ikke være perfekt, den vil på intervallet $(1+\delta)^{-1}x\le n<(1+\delta)x$ dekke litt mer enn vi egentlig vil. For dette området trenger vi da et eget estimat.

Lemma 29. *La Γ være intervallet $[(1+\delta)^{-1}x,(1+\delta)x)$. Da har vi*

$$\sum_{\substack{n\in\Gamma\\ n\equiv a\,(\mathrm{mod}\,q)}}\sum_{\substack{x^{1/5}<m\le x^{4/5}\\ lm=n}}\lambda(l)\mu(m)-\frac{1}{\phi(q)}\sum_{\substack{n\in\Gamma\\ (n,q)=1}}\sum_{\substack{x^{1/5}<m\le x^{4/5}\\ lm=n}}\lambda(l)\mu(m)$$

$$\ll\delta q^{-1}x\log^2 x.$$

Bevis. Vi lar la Γ_m være tilsvarende intervall som Γ, men hvor x er byttet ut med x/m. Ved å endre på på summasjonen på samme måte som vi gjorde i lemma 28 kan vi få

$$\sum_{\substack{n\in\Gamma\\ n\equiv a\,(mod\,q)}}\sum_{\substack{x^{1/5}<m\le x^{4/5}\\ lm=n}}\lambda(l)\mu(m)-\frac{1}{\phi(q)}\sum_{\substack{n\in\Gamma\\ (n,q)=1}}\sum_{\substack{x^{1/5}<m\le x^{4/5}\\ lm=n}}\lambda(l)\mu(m)$$

$$=\sum_{\substack{x^{1/5}<m\le x^{4/5}\\ (m,q)=1}}\mu(m)\sum_{\substack{l\in\Gamma_m\\ l\equiv am^{-1}\,(mod\,q)}}\lambda(l)-\frac{1}{\phi(q)}\sum_{\substack{x^{1/5}<m\le x^{4/5}\\ (m,q)=1}}\mu(m)\sum_{\substack{l\in\Gamma_m\\ (l,q)=1}}\lambda(l).$$

Enkle estimater på de indre summene gjør at vi kan få disse

$$\begin{aligned}&\ll\sum_{\substack{x^{1/5}<m\le x^{4/5}\\ (m,q)=1}}\frac{|\mu(m)|\delta x\log x}{mq}\\ &\ll\ \delta q^{-1}x\log^2 x,\end{aligned}$$

hvor vi i slutten her har brukt at $\sum_{m\le x}m^{-1}\ll\log x$. □

Lar vi nå $D(LM;q,a)$ være summen

$$\sum_{\substack{l,m\\ L<l\le(1+\delta)L\\ M<m\le(1+\delta)M\\ lm\equiv a\,(mod\,q)}}\lambda(l)\mu(m)-\frac{1}{\phi(q)}\sum_{\substack{l,m\\ L<l\le(1+\delta)L\\ M<m\le(1+\delta)M\\ (lm,q)=1}}\lambda(l)\mu(m),\tag{2.35}$$

har vi

$$D_{\Lambda^\sharp}(x;q,a)=\sum_{L,M}D(LM;q,a)+O(\delta q^{-1}x\log^2 x).\tag{2.36}$$

Det eneste som gjenstår før vi kan bruke teorem 21 på intervallene vi nå har snakket om, er å vise at $\mu(m)$ oppfyller kravet i (2.20).

Lemma 30. *For $\beta_n=\mu(n)$ har vi*

$$|D_\beta(x;q,a)|\ll\|\vec{\beta}\|x^{\frac{1}{2}}\Delta^9$$

med $\Delta^9=\log^{-A}x$.

Bevis. Fra [MV07, teorem 2.2] vet vi at

$$\sum_{n\le x}|\mu(n)|^2=\frac{6}{\pi^2}x+O(x^{1/2})\gg x$$

slik at

$$\|\vec{\mu}\|=\Big(\sum_{n\le x}|\mu(n)|^2\Big)^{1/2}\gg x^{1/2}.$$

Dette betyr at $\|\vec{\mu}\|x^{1/2}\log^{-A}x \gg x\log^{-A}x$, som betyr at om man har $|D_\mu(x;q,a)| \ll x\log^{-A}x$, har man også $|D_\mu(x;q,a)| \ll \|\vec{\mu}\|x^{1/2}\log^{-A}x$. Ved ortogonalitet kan vi skrive

$$\sum_{\substack{n\leq x\\ n\equiv a\,(\mathrm{mod}\,q)}}\mu(n) = \frac{1}{\phi(q)}\sum_{\chi\,(\mathrm{mod}\,q)}\Big(\sum_{n\leq x}\chi(n)\mu(n)\Big),$$

hvor summen her er over alle Dirichlet-karakterer modulo q. Om vi nå på høyresiden trekker den trivielle karakteren χ_0 ut av summen, har vi

$$\sum_{\substack{n\leq x\\ n\equiv a\,(\mathrm{mod}\,q)}}\mu(n) = \frac{1}{\phi(q)}\sum_{\substack{n\leq x\\ (n,q)=1}}\mu(n) + \frac{1}{\phi(q)}\sideset{}{^\bullet}\sum_{\chi\,(\mathrm{mod}\,q)}\Big(\sum_{n\leq x}\chi(n)\mu(n)\Big),$$

hvor $\sum^\bullet$ betyr at vi summerer over alle ikke trivielle Dirichlet-karakterer modulo q. Betingelsen $(n,q)=1$ i første sum på høyre side kan vi legge til da $\chi(n)=0$ for alle $(n,q)\neq 1$. Videre vil da

$$\sum_{\substack{n\leq x\\ n\equiv a\,(\mathrm{mod}\,q)}}\mu(n) - \frac{1}{\phi(q)}\sum_{\substack{n\leq x\\ (n,q)=1}}\mu(n) = \frac{1}{\phi(q)}\sideset{}{^\bullet}\sum_{\chi\,(\mathrm{mod}\,q)}\Big(\sum_{n\leq x}\chi(n)\mu(n)\Big),$$

slik at

$$D_\mu(x;q,a) = \frac{1}{\phi(q)}\sideset{}{^\bullet}\sum_{\chi\,(\mathrm{mod}\,q)}\Big(\sum_{n\leq x}\chi(n)\mu(n)\Big).$$

Fra [IK04, likning 5.80] vet vi at vi for alle primitive Dirichlet-karakterer χ modulo q med $q>2$ har

$$\sum_{n\leq x}\chi(n)\mu(n) \ll \sqrt{q}x\log^{-A}x$$

for enhver $A>0$. Dette gir da at

$$D_\mu(x;q,a) \ll \sqrt{q}x(\log x)^{-A} + \frac{1}{\phi(q)}\sideset{}{^{\bullet\bullet}}\sum_{\chi\,(\mathrm{mod}\,q)}\Big(\sum_{n\leq x}\chi(n)\mu(n)\Big)$$

hvor $\sum^{\bullet\bullet}$ betyr at vi summerer over alle ikke trivielle og imprimitive Dirichlet-karakterer, og vi har brukt at antallet primitive karakterer modulo q er $\leq\phi(q)$ (dette gjelder for alle karakterer). Alle imprimitive karakterer χ modulo q er indusert av en unik primitiv karakter χ_i modulo d, hvor $d|q$. Den eneste forskjellen mellom χ og χ_i er at χ forsvinner på flere tall enn det χ_i gjør. Derfor har vi at $\chi(n)\leq\chi_i(n)$, og i summen $\sum^{\bullet\bullet}$ kan vi bytte ut χ-ene med χ_i-er og få en ulikhet. Altså har vi

$$\frac{1}{\phi(q)}\sideset{}{^{\bullet\bullet}}\sum_{\chi\,(\mathrm{mod}\,q)}\Big(\sum_{n\leq x}\chi(n)\mu(n)\Big) \leq \frac{1}{\phi(q)}\sum_{\chi_i}^{i}\Big(\sum_{n\leq x}\chi_i(n)\mu(n)\Big)$$

hvor vi nå har byttet ut summen $\sum^{\bullet\bullet}$ med summen av de induserende (primitive) karakterene χ_i. Slår vi sammen har vi nå

$$\begin{aligned} D_\mu(x;q,a) &\ll \sqrt{q}x\log^{-A}x + \frac{1}{\phi(q)}\sum_{\chi_i}\Big(\sum_{n\le x}\chi_i(n)\mu(n)\Big) \\ &\ll \sqrt{q}x\log^{-A}x + \sqrt{q}x\log^{-A}x \ll \sqrt{q}x\log^{-A}x. \end{aligned}$$

Videre vet vi at estimatet

$$D_f(x;q,a) \ll \Big(\sum_{n\le x}|f(n)|^2\Big)^{1/2}x^{1/2}\log^{-C}x$$

er ikke-trivielt kun for $q \ll \log^C x$, for om q skulle gå mot uendelig som en n-te-rot av x (for eksempel), ville $\phi(q)$[3] vokst så fort at feilleddet ble trivielt. Vi kan derfor anta at $q \ll \log^C x$ slik at $\sqrt{q}x\log^{-A}x \ll x\log^{-A}x$. Dette betyr at $|D_\mu(x;q,a)| \ll x\log^{-A}x \ll \|\vec{\mu}\|x^{1/2}\log^{-A}x$, og velger vi nå A slik at $\Delta^9 = \log^{-A}x$ (det vil komme frem senere ved valget av Δ at vi faktisk kan velge A slik) er vi i mål . □

Vi kan nå estimere $|D_{\Lambda^\flat}(x,q,a)|$ ved å bruke teorem 21 på de $O(\delta^{-2}\log^2 x)$ intervallene i (2.35). Dette vil være den siste brikken i beviset av teorem 4.

Bevis for teorem 4. Vi velger nå $Q = \Delta x^{1/2}$ og tar med oss at

$$\|\vec{\alpha'}\|^2 \le \delta M, \|\vec{\beta'}\|^2 \le \delta L\log^2 x \text{ og } \log Q \ll \log x,$$

hvor $\vec{\alpha'}$ er $\mu(m)$ restriktert til $M < m \le (1+\delta)M$ og $\vec{\beta'}$ er $\beta(l)$ restriktert til $L < l \le (1+\delta)L$. Da gir teorem 21 oss at

$$\sum_{q\le Q}\max_{(a,q)=1}|D(LM;q,a)|$$

$$\begin{aligned} &\ll \|\vec{\alpha'}\|\|\vec{\beta'}\|(\Delta(\delta M)^{1/2}(\delta L)^{1/2} + (\delta M)^{1/2} + (\delta L)^{1/2} + Q)\log^2 Q \\ &\ll (\delta M)^{1/2}(\delta L)^{1/2}\log x(\Delta(LM)^{1/2} + L^{1/2} + M^{1/2} + \Delta x^{1/2})\log^2 x \\ &\ll \delta\Delta x\log^3 x, \end{aligned}$$

da $\delta \le 1$ og $L, M, LM < x$. Summerer vi nå over de $O(\delta^{-2}\log^2 x)$ slike L, M og tar med oss feilleddet fra (2.36) , får vi

$$\sum_{q\le Q}\max_{(a,q)=1}|D_{\Lambda^\flat}(x;q,a)| \ll \delta^{-1}\Delta x\log^5 x + \delta x\log^3 x,$$

hvor vi har brukt $\sum_{q\le Q}\frac{1}{q} \ll \log Q \le \log x$. Setter vi nå $\delta = \Delta^{1/2}\log x$, blir begge utrykkene lik

$$\Delta^{1/2}x\log^4 x.$$

[3]Den nedre grensen for $\phi(q)$ er proporsjonal med $n/\log\log n$.

Fra (2.33) har vi nå da at

$$\sum_{q\leq Q}\max_{(a,q)=1}|D_\Lambda(x;q,a)| = \sum_{q\leq Q}\max_{(a,q)=1}\left|\psi(x;q,a)-\frac{1}{\phi(q)}\sum_{\substack{n\leq x\\(n,q)=1}}\Lambda(n)\right|$$

$$\begin{aligned}
&= \sum_{q\leq Q}\max_{(a,q)=1}|D_{\Lambda^\sharp}(x;q,a)| + \sum_{q\leq Q}\max_{(a,q)=1}|D_{\Lambda^\flat}(x;q,a)| + O(x^{1/5}\log x)\\
&\ll Qx^{2/5} + \Delta^{1/2}x\log^4 x + O(x^{1/5}\log x)\\
&= \Delta x^{9/10} + \Delta^{1/2}x\log^4 x + O(x^{1/5}\log x).
\end{aligned}$$

Velger vi nå $\Delta = \log^{-B} x$ har vi da

$$\begin{aligned}
\sum_{q\leq Q}\max_{(a,q)=1}|D_\Lambda(x;q,a)| &\ll x^{9/10}\log^{-B}x + x\log^{4-\frac{B}{2}}x + O(x^{1/5}\log x)\\
&\ll x\log^{4-\frac{B}{2}}x.
\end{aligned}$$

Fra Primtallsteoremet tar vi med oss at

$$\sum_{\substack{n\leq x\\(n,q)=1}}\Lambda(n) = \psi(x) = x + O(x\log^{-C}x),$$

slik at

$$\sum_{q\leq Q}\max_{(a,q)=1}|D_\Lambda(x;q,a)| = \sum_{q\leq Q}\max_{(a,q)=1}\left|\psi(x;q,a)-\frac{x}{\phi(q)}-O(\frac{x\log^{-C}x}{\phi(q)})\right|$$

$$\leq \sum_{q\leq Q}\max_{(a,q)=1}\left|\psi(x;q,a)-\frac{x}{\phi(q)}\right| + O\left(\sum_{q\leq Q}\frac{1}{\phi(q)}(x\log^{-C}x)\right).$$

Her bruker vi (2.29) slik at utrykket vårt blir

$$\ll \sum_{q\leq Q}\max_{(a,q)=1}\left|\psi(x;q,a)-\frac{x}{\phi(q)}\right| + O(\log(x^{1/2}\log^{-B}x)(x\log^{-C}x)).$$

Feilleddet blir her dominert av $x\log^{4-\frac{B}{2}}x$ slik at man tilslutt ender med

$$\sum_{q\leq Q}\max_{(a,q)=1}\left|\psi(x;q,a)-\frac{x}{\phi(q)}\right| \ll_A x\log^{4-\frac{B}{2}}x,$$

som gir oss Bombieri-Vinogradovs teorem for $B(A) = 2A + 8$[4]. □

Vi er nå ferdig med hoveddelen av denne oppgaven, og avslutter med et kapittel om primtallsgap hvor vi vil snakke litt om hvorfor Bombieri-Vinogradovs teorem er så viktig. Mye av informasjonen i kapittelet om primtallsgapene er hentet fra [Tao14].

[4]Dette er ikke samme A som i lemma 30.

Kapittel 3

Primtallsgap

I april 2013 overrasket Yitang Zhang [Zha14] matematikkverden ved å hevde at han hadde et bevis for at det fantes et tall $k < 7 \times 10^7$, slik at det finnes uendelig mange par av primtall på formen $p, p + k$. Det tok omtrent en måneds tid før beviset var godkjent av **Annals of Mathematics,** og det var klart at den relativt ukjente matematikeren hadde kommet med et meget oppsiktsvekkende resultat. Dette resultatet er et steg i retning et av de store uløste matematiske problemene, nemlig Tvillingprimtallsformodningen. Tvillingprimtallsformodningen vil være Zhangs resultat for $k = 2$, og selv om 70 000 000 er ganske langt fra 2, var det for matematikere forløsende å ha endelighet.

3.1 Goldston-Pintz-Yildirim

Zhangs arbeid bygger på et gjennombrudd av Goldston, Pintz og Yildirim [GPY09] fra 2005. De var de første til å bruke Selbergs såldmetode på ekvidistrubisjonsestimater for primtallene for å få kontroll på størrelsen av primtallsgap. Bombieri-Vinogradovs teorem er et ekvidistrubisjonsetimat for primtallene. Med dette mener vi et estimat som begrenser feilleddet mellom antallet primtall i en gitt aritmetisk progresjon, og gjennomsnittet over alle aritmetiske progresjoner. For å enklere kunne forklare hva som ble gjort av Goldston, Pintz og Yildirim, introduserer vi to nye begreper.

Definisjon. Hvis p_n er det n-te primtallet, skriver vi

$$H_m \coloneqq \liminf_{n\to\infty} p_{n+m} - p_n.$$

Og vi tar med en generalisering av Bombieri-Vinogradovs teorem.

Definisjon (Elliott-Halberstam)**.** For $0 < \theta < 1$ sier vi at vi har Elliott-Halberstam på nivå θ (forkortes EH[θ]) om følgende holder for alle $A > 0$

$$\sum_{q\leq x^\theta} \max_{(a,q)=1} |E(x;q,a)| \ll_A x \log^{-A} x,$$

hvor Elliott-Halberstam-formodningen er at dette holder for alle $\theta < 1$.

Vi legger da merke til at EH$[\frac{1}{2} - \epsilon]$ tilsvarer Bombieri-Vinogradovs teorem. Det Goldston, Pintz og Yildirim viste, var at de ved hjelp av Bombieri-Vinogradovs teorem kunne få $\liminf_{n\to\infty} \frac{p_{n+m} - p_n}{\log p_n} = 0$. Sagt på en annen måte sier dette at det finnes uendelig mange primtall, hvor vi kan få avstanden til det neste primtallet til å bli så liten vi bare vil i forhold til den gjennomsnittelige avstanden mellom påfølgende primtall (som vil være omtrent $\log x$ for primtall av størrelse x). Videre viste GPY også at enhver forbedring av Elliott-Halberstam på formen EH$[\frac{1}{2} + \varpi]$ for $\varpi > 0$, ville gi endelighet for H_1. Om de antok EH$[\theta]$ for alle $\theta < 1$, fikk de imidlertid begrensningen helt ned til $H_1 \leq 16$.

3.2 Zhangs arbeid

Selv om disse resultatene satt i gang en ny måte å angripe problemet på, gikk det nesten ti år før det neste store gjennombruddet kom med Zhang i 2013. Zhangs resultat kan omformuleres til at $H_1 \leq 70\,000\,000$, og med det var han første person til å bevise endelighet for H_1. I sitt arbeid hadde Zhang tatt seg store friheter med konstantene sine, og han hadde vært slapp med estimatene, da hans eneste mål var å få en endelig grense. Det tok derfor ikke lang tid fra Zhangs arbeid ble utgitt, til matematikere verden over kastet seg på for å stramme inn både estimater og argumenter slik at de, om bare for en dag, kunne påstå seg å ha rekorden for beste begrensning. Det Zhang gjorde for å få resultatet sitt, var å bevise en litt svakere versjon av EH[1/2].

Definisjon. For et par $\varpi, \delta > 0$ har man MPZ$[\varpi, \delta]$ (etter Motohashi, Pintz og Zhang) om følgende holder

$$\sup_{\substack{a \\ (a,p)=1 \\ \forall p \leq x^{\delta}}} \sum_{\substack{q \leq x^{1/2+2\varpi} \\ q \text{ er kvadratfri} \\ q \text{ er } x^{\delta}\text{-glatt}}} \left| \sum_{\substack{n \equiv a \,(mod\, q) \\ n \leq x}} \Lambda(n) - \frac{1}{\phi(q)} \sum_{\substack{(n,q)=1 \\ n \leq x}} \Lambda(n) \right| \ll_A x \log^{-A} x.$$

Hvor x^{δ}-glatt betyr at alle primfaktorene til q er mindre eller like x^{δ}.

Det hadde vært klart siden GPY at ethvert bevis av MPZ$[\varpi, \delta]$ ville gi endelighet for H_1, og det var dette Zhang var den første til å bevise for verdier $\varpi = \delta = \frac{1}{1168}$.

Primtupler

Når man oppnår resultater om primtallsgapene er det som oftest ved å begrense størrelsen på en spesiell type tuppel som inneholder et visst antall primtall. En primtallstuppel (eller en **prim k-tuppel**) er en tuppel med heltall av lengde k

$$h_1 < h_2 < \cdots < h_k. \tag{3.1}$$

Poenget med disse tuplene, er å «matche» gap mellom primtallene, og vanligvis er det slik at h_1 settes til 0 og de resterende verdiene er positive heltall. Når man jobber med primtupler, er det som oftest **tillate** primtupler man arbeider med. En tillat primtuppel er en tuppel der h_i-ene unngår minst en restklasse mod$p$ for alle primtall p . For eksempel er $(0, 2, 4)$ ikke en tillat primtuppel, da den inneholder alle restklasser $\bmod 3$. Dette betyr at $n+0, n+2, n+4$ ikke alle kan være primtall samtidig (bortsett fra et endelig antall ganger), mens derimot $(0, 2, 6)$ eller $(0, 4, 6)$ er tillate primtupler. Når man snakker om størrelsen til en primtuppel, brukes begrepet diameter som er differansen mellom første og siste element. Dette gir naturlig opphav til en funksjon $H(k)$ som er den minste diameteren en tillat prim $k-$tuppel kan ha. Vi har da allerede sett at $H(3) = 6$, og neste steg i rekken blir $H(4) = 8$ med tuppel $(0, 2, 6, 8)$. Disse tallene forstår man ganske godt, og man har ved hjelp av datamaskiner regnet ut $H(k)$ for k i underkant av 350. Det er formodet av Hardy og Littlewood at $H_m = H(m+1)$, men dette er et resultat som ser ut til å ligge en god del dypere enn det man kan dykke i dag. En annen formodning av Hardy og Littlewood (denne gang i sammarbeid med Dickson) må også å nevnes i denne sammenhengen. Man sier at man har DHL$[k, j]$ for $k, j \in \mathbb{N}$ med $j \leq k$ om det for alle tillate k-tupler på formen (3.1) finnes uendelig mange forskyvninger $n + h_1 < \cdots < n + h_k$, slik at disse tallene inneholder minst j primtall. Hadde man for eksempel hatt DHL$[2, 2]$, ville dette implisert Tvillingprimtallsformodningen. Da Zhang fikk sitt resultat, viste han at DHL$[k_0, 2]$ holdt for alle $k_0 \geq 3.5 \times 10^6$. Om man velger de første k_0 primtallene større enn k_0, vil man få en tillat k_0-tuppel. Ulikheten $\pi(7 \times 10^7) - \pi(3.5 \times 10^6) > 3.5 \times 10^6$ gjorde da at Zhang trygt kunne velge sin k til å være 7×10^7. [1]

3.3 Polymath og Maynard

Det tok som sagt ikke lang tid fra Zhangs arbeid ble publisert, til matematikere begynte å jobbe med å presse Zhangs konstant nedover. Etter en liten periode valgte matematikerene som jobbet med dette å slå seg sammen i et prosjekt kalt Polymath8, ledet av Terrence Tao. Sammen klarte man etter ikke mange måneder å presse Zhangs konstant helt ned til 4680, ved å forbedre Zhangs verdier til $\varpi < \frac{6}{700} - \frac{9}{35}\delta$ for $\delta > 0$. Det så ut til at denne verdien skulle bli stående en god stund, men bare måneder senere kom James Maynard opp med en helt ny metode som kunne presse konstanten ned til 600, en betraktelig forbedring. Istedenfor å prøve å forbedre ekvidistrubisjonsargumentet, forandret Maynard heller såldmetoden som ble brukt. Han gikk fra et endimensjonalt Selberg såld, til et flerdimensjonalt som førte til ganske oppsiktsvekkende resultater. Ikke bare fikk han en bedre begrensning for H_1, men han klarte også som første å begrense H-ene av høyere grad. Han viste at for alle $m \leq 1$, så holder $H_m \ll m^3 e^{2m}$, altså endelighet for alle m. Dette er fortsatt langt fra $m \log m$ som forventes å være det korrekte, men Maynards metode gjorde at

[1] Ulikheten holder også ned til 64 millioner, men jeg antar Zhang synes 70 var et finere tall å bruke.

man endelige også kunne kontrollere H-ene av høyere grad. Under antakelsen av Elliott-Halberstam-formodningen klarte han også å trimme GPYs resultat for H_1 ned til 12. Maynard valgte deretter og slå meg sammen med Polymath-gruppen under sideprosjektet Polymath8b. Sammarbeidet viste seg å gi frukter. Da gruppen i juni 2014 så seg ferdig med prosjektet [Pol14], hadde man opparbeidet seg flere gode resultater. Man hadde blant annet vist at DHL$[50, 2]$ holder, noe som gir en begrensning helt ned til $H_1 \leq 246$. Det finnes nemlig en tillat 50-tuppel av diameter 246, og man har ved hjelp av datamaskiner sjekket at dette er optimalt for en tuppel av den størrelsen. For H-ene av høyere grad gav prosjektet også en liten forbedring av Maynards originale resultat. De fikk $H_m \ll me^{(4-\frac{28}{157})m}$, selv om dette fortsatt er eksopensielt i m . Disse resultatene var ubetinget (kun avhengig av Bombieri-Vinogradovs teorem), men betinget kunne man få enda sterkere resultater. Ved å anta den generaliserte Elliott-Halberstam-formodningen[2] (GEH), kunne man komme helt ned til $H_1 \leq 6$. I generaliseringen av Elliott-Halberstam har man byttet fra å summere over Von Mangoldt-funksjonen, til å summere over en Dirichlet-konvulsjon av to aritmetiske følger som man tillegger visse begrensninger. På samme måte som tidligere, så er denne begrensningen av H_1 oppnådd ved å jobbe med primtupler. Polymath-gruppen viste at GEH gir DHL$[3, 2]$, med $H_1 \leq 6$ (velg tuppel $(0, 2, 6)$ eller $(0, 4, 6)$). Men DHL$[3, 2]$ har også en annen morsom konsekvens. La N være et tilstrekkelig stort multippel av 6, og se på tuppelen $(n, n + 2, N - n)$. Dette vil være en tillat primtuppel, og DHL$[3, 2]$ forteller oss da at den vil inneholde minst 2 primtall for uendelig mange n. Dette gir oss en fiffig adjunksjon. Enten må Tvillingprimtallsformodningen holde, eller så må alle store partall være maksimalt 2 fra et Goldbach-tall[3] (det forventes selvfølgelig at begge utsagnene er korrekte). Dette kan vi si da vi enten har at paret $n, n + 2$ er prim uendelig mange ganger, eller så vil et av parene $n, N - n$ og $n + 2, N - n$ være det. Antar vi at vi ikke har uendelig mange primtallstvillinger, vil enten N eller $N + 2$ være en sum av to primtall. Alle partall er enten et multippel av 6, eller på formen $N \pm 2$ hvor N er et multippel av 6. Om tallet skulle være på formen $N - 2$, kan vi bare forandre andre element i tuppelene vår fra $n + 2$ til $n - 2$, og vi har da garantert oss at alle tilstrekkelige store partall vil være innenfor 2 fra å være en sum av to primtall.

3.4 Selbergs paritetsproblem

Når man under antakelsen av GEH kan få H_1 øvrig begrenset av 6, kan det virke som om man er på god vei mot Tvillingprimtallsformodningen. Derimot finnes det en obstruksjon som gjør det umulig (tror man) å bevise at $H_1 \leq 4$ kun ved hjelp av såldmetoder. Vi vil her gjengi en forenklet versjon av den har i [Pol14] for å forklare denne problemstillingen. Atle Selberg[Sel52] viste at det var visse begrensninger for såldmetodene, og at ikke alle problemer kan løses

[2] GEH er sterkere og vil implisere EH.

[3] Et Goldbach-tall er et partall som kan skrives som summen av to primtall, og Goldbach-formodningen påstår at alle partall større enn 2 er Goldbach-tall.

kun ved hjelp av disse metodene. Polymath8b fant som nevnt $H_1 \leq 6$ ved å vise at DHL$[3,2]$ holder under antagelsen av GEH. Dette er det samme som å vise at mengden $A = \{n \in \mathbb{N} : \text{ minst to av } n, n+2, n+6 \text{ er prim}\}$ er uendelig. For å kunne vise dette, opparbeidet de seg en nedre begrensning slik at

$$\sum_n \nu(n)\mathbf{1}_A(n) > 0$$

for en ikke-negativ vektfunksjon $\nu : \mathbb{N} \to \mathbb{R}^+$ støttet på et intervall $[x, 2x]$ for passende stor x. Denne nedre begrensningen fikk de ved å ha gode estimater for differanser lignende de vi har sett på tidligere

$$\Big| \sum_{\substack{x\leq n\leq 2x \\ n=a \,(mod\, q)}} f(n+h) - \frac{1}{\phi(q)} \sum_{\substack{x\leq n\leq 2x \\ (n+h,q)=1}} f(n+h)\Big|, \tag{3.2}$$

for alle $h \in \{0, 2, 6\}$, forskjellige restklasser modulo q med $q \leq x^{1-\epsilon}$ og en rekke forskjellige aritmetiske funksjoner. Man har oppdaget at de samme argumentene vil fungere om man introduserer enda en ikke-negativ vektfunksjon $\omega : \mathbb{N} \to \mathbb{R}^+$, og man kan utlede en nedre begrensning på formen

$$\sum_n \nu(n)\mathbf{1}_A(n)\omega(n) > 0,$$

om man har kontroll på den vektede differansen

$$\Big| \sum_{\substack{x\leq n\leq 2x \\ n=a \,(mod\, q)}} f(n+h)\omega(n) - \frac{1}{\phi(q)} \sum_{\substack{x\leq n\leq 2x \\ (n+h,q)=1}} f(n+h)\omega(n)\Big|. \tag{3.3}$$

Dersom man skulle vise at $H_1 \leq 4$ ved hjelp av såldmetoder, ville det være nærliggende å prøve å bytte ut A med

$$A' = \{n \in \mathbb{N} : n, n+2 \text{ begge tall er prim}\} \cup \{n \in \mathbb{N} : n+2, n+6 \text{ begge tall er prim}\}.$$

For deretter å håpe på å få en nedre begrensning på formen

$$\sum_n \nu(n)\mathbf{1}_{A'}(n) > 0$$

for en nøye valgt funksjon $\nu : \mathbb{N} \to \mathbb{R}^+$ støttet på intervallet $[x, 2x]$, utledet fra passende begrensinger av summer på samme form som i (3.2). Om dette var gjort kun ved hjelp av såldmetoder, kunne man også fått den nedre begrensningen

$$\sum_n \nu(n)\mathbf{1}_{A'}(n)\omega(n) > 0 \tag{3.4}$$

for enhver ikkenegativ vektfunksjon $\omega : \mathbb{N} \to \mathbb{R}^+$, gitt at man hadde samme kontroll på differansene som i (3.3) . Om vi velger $\omega(n)$ slik at

$$\begin{aligned}\omega(n) &\coloneqq (1 - \lambda(n)\lambda(n+2))(1 - \lambda(n+2)\lambda(n+6)) \\ &= 1 - \lambda(n)\lambda(n+2) - \lambda(n+2)\lambda(n+6) + \lambda(n)\lambda(n+6)\end{aligned}$$

hvor $\lambda(n) = (-1)^{\Omega(n)}$ er Liouville-funksjonen, ser vi at $\omega(n) = 0$ for alle $n \in A'$, og derfor vil

$$\sum_n \nu(n)\mathbf{1}_{A'}(n)\omega(n) = 0 \tag{3.5}$$

for alle ν. Nå har det seg slik at Möbius' tilfeldighetslov (eller Liouvilles tilfeldighetslov i vårt tilfelle) forventer mye kansellasjon i summer som innvolverer fortegnsbytte hos $\lambda(n)$, der de andre faktorene ikke direkte avhenger av primtallsfaktoriseringen av n. For eksempel burde

$$\sum_{n \leq x} a_n \lambda(n)$$

være «relativt» liten grunnet kansellasjon, om a_n er en rimelig valgt følge (rimelig i den betydning at følgen er valgt uten bias). Hvis vi setter inn $\omega(n)$ i (3.2), vil vi få summer på formen

$$\sum_{\substack{x \leq n \leq 2x \\ n = a \,(mod\, q)}} f(n+h)\lambda(n)\lambda(n+2).$$

Disse summene forventes å bli så små at de ikke bidrar nevneverdig i feilleddet, slik at om man har godt grep om differanser som på formen i (3.2) , har man også kontroll på de vektede differansene. Vi konkluderer derfor med at alle begrensninger for differanser av typen i (3.2), også (sannsynligvis) vil holde på formen (3.3). Dette betyr at om man har vist at $H_1 \leq 4$ ved hjelp av såldmetoder, burde man også kunne få et resultat som (3.4), men dette motsier (3.5). Skal man angripe Tvillingprimtallsformodningen, kan det derfor virke lurt å ha noen nye verktøy i beltet.

Bibliografi

[Ahl66] Lars V. Ahlfors. *Complex analysis: An introduction of the theory of analytic functions of one complex variable*. Second edition. McGraw-Hill Book Co., New York-Toronto-London, 1966. 2.1

[Aub87] Karl Egil Aubert. *Innføring i tallteori*. Matematisk Institutt, Universitetet I Oslo, 1987. 2.3

[BD69] E. Bombieri and H. Davenport. Some inequalities involving trigonometrical polynomials. *Ann. Scuola Norm. Sup. Pisa (3)*, 23:223–241, 1969. 2.2

[Bom65] E. Bombieri. On the large sieve. *Mathematika*, 12:201–225, 1965. 2

[GPY09] Daniel A. Goldston, János Pintz, and Cem Y. Yıldırım. Primes in tuples. I. *Ann. of Math. (2)*, 170(2):819–862, 2009. 3.1

[Har11] Nick Harland. Large sieve and Bombieri-Vinogradov theorem, `http://www.math.ubc.ca/~gerg/teaching/613-winter2011/largesievebombierivinogradov.pdf`, 2011. (document)

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004. 2.3, 2.3

[MV74] H. L. Montgomery and R. C. Vaughan. Hilbert's inequality. *J. London Math. Soc. (2)*, 8:73–82, 1974. 2.1

[MV07] Hugh L. Montgomery and Robert C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007. 1.2, 2.3

[Pol09] Paul Pollack. *Not always buried deep*. American Mathematical Society, Providence, RI, 2009. A second course in elementary number theory. 2.2.1, 2.3

[Pol14] D. H. J. Polymath. Variants of the Selberg sieve, and bounded intervals containing many primes. *Res. Math. Sci.*, 1:1:12, 2014. 3.3, 3.4

[Sel52] Atle Selberg. On elementary methods in primenumber-theory and their limitations. In *Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949*, pages 13–22. Johan Grundt Tanums Forlag, Oslo, 1952. 3.4

[Sel91] Atle Selberg. *Collected papers. Vol. II.* Springer-Verlag, Berlin, 1991. With a foreword by K. Chandrasekharan. 2.1

[Tao14] Terrence Tao. Bounded gaps between primes 1–3, `https://www.youtube.com/watch?v=huiskxcghck`, 2014. Lectures at the IHÉS Summer School on analytic number theory. 2.3

[Vin65] A. I. Vinogradov. The density hypothesis for Dirichet L-series. *Izv. Akad. Nauk SSSR Ser. Mat.*, 29:903–934, 1965. 2

[Wal36] Arnold Walfisz. Zur additiven Zahlentheorie. II. *Math. Z.*, 40(1):592–607, 1936. 1.2

[Zha14] Yitang Zhang. Bounded gaps between primes. *Ann. of Math. (2)*, 179(3):1121–1174, 2014. 3